

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

IN RE: DEALER MANAGEMENT SYSTEMS
ANTITRUST LITIGATION

MDL No. 2817
Case No. 18 C 864

This Document Relates to:
Authenticom, Inc. v. CDK Global, LLC, et al.,
Case No. 1:18-cv-00868 (N.D. Ill.)

Hon. Robert M. Dow, Jr.
Magistrate Judge Jeffrey T. Gilbert

PUBLIC-REDACTED

**AUTHENTICOM, INC.'S ANSWER AND AFFIRMATIVE AND OTHER DEFENSES
TO DEFENDANT AND COUNTER-PLAINTIFF THE REYNOLDS AND REYNOLDS
COMPANY'S COUNTERCLAIMS**

1. The Reynolds and Reynolds Company expended enormous resources building and maintaining a high-end, highly-integrated, closely-controlled enterprise software and computing platform for automotive dealerships and dealership groups. In the industry, enterprise platforms for automotive dealerships are known as Dealer Management Systems or, more commonly, DMSs. The Reynolds DMS is a bespoke product and comprises more than 20 million lines of programming code. Today, the Reynolds DMS is distributed across more than 5,000 automobile dealers in North America, requiring constant maintenance, control, and monitoring of a complex, distributed computing network that Reynolds created, built, refined, improved and scaled over decades to achieve maximum performance, speed, stability and security.

ANSWER: Authenticom, Inc. ("Authenticom") admits that The Reynolds and Reynolds Company ("Reynolds") provides enterprise software known as dealer management systems ("DMS") and related services. Authenticom admits that Reynolds's DMS provides dealers with software tools and resources necessary to manage core aspects of their business. Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 1 of the Counterclaims that relate to the details of Reynolds's products or Reynolds's

internal expenditures, development costs, and customer base, and on that basis denies them.

Authenticom denies the remaining allegations in Paragraph 1.*

2. For these reasons, among others, the Reynolds DMS is a premium product that commands a premium price. Reynolds licenses its DMS to its dealership customers under a strict set of terms and conditions designed to protect its system's functional integrity and security, protect Reynolds's valuable intellectual property rights, and meet Reynolds's contractual obligations to third parties. As a condition of this license, each Reynolds dealer agrees that the only persons allowed to access and use the DMS shall be dealership employees who use the DMS on a day-to-day basis to carry out their job functions. Dealers know and agree to this restriction (and others) when they choose to license a Reynolds DMS, and both Reynolds and the dealers negotiate the resulting licensing fees based on the expectation that the license's scope extends to dealership employees alone.

ANSWER: Paragraph 2 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom admits that Reynolds's product is one of the most expensive in the DMS market. Authenticom admits that Reynolds licenses have numerous provisions, but denies that the provisions are designed to protect system functional integrity and security, protect Reynolds's intellectual property, or meet contractual relationships with third parties, but instead are designed to further Reynolds's anticompetitive purposes. Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 2 of the Counterclaims that relate to Reynolds contract negotiations, and on that basis denies them. Authenticom denies the remaining allegations of Paragraph 2.

3. Reynolds's DMS is a premium product because it is significantly more stable, secure, and effective than similar products provided by its competitors. Though there are tens of thousands of new and used car dealerships in the United States, Reynolds sells its proprietary DMS primarily to larger car dealership groups that require a sophisticated, stable, and secure platform to manage the complex network of transactions (and vast cashflows) that move through their businesses. Reynolds's DMS gives these dealers numerous tools and functionalities that allow them to improve the profitability and efficiency of their operations.

ANSWER: Denied.

* To the extent the headings or other content in the Counterclaims not contained in numbered paragraphs, such as section headings, are considered allegations within the pleading, Authenticom denies them.

4. Dealership operations, particularly those of Reynolds's target customers, generate and depend upon a swathe of critically sensitive private data, including consumer financial information far more detailed and voluminous than ordinary consumer transactions. By way of example, that information frequently includes credit scores, driver's license numbers, and Social Security Numbers. Protecting the integrity and security of the Reynolds platform, and the sensitive consumer financial data it contains, is a paramount concern for both Reynolds and its customers. Consistent with this concern, Reynolds's system includes multiple protections designed to exclude hackers, to prevent automated scripts from encumbering system resources, and to ensure that only properly licensed dealership employees can access and use the system.

ANSWER: Authenticom admits that some dealership operations generate information about consumer transactions. Authenticom denies that Reynolds's actions in intentionally disrupting Authenticom's business activities is related to a concern for Reynolds's customers or the sensitivity of the information described in Paragraph 4. Authenticom denies that Reynolds's purported "protections" are related to providing value to customers or protecting the integrity or security of Reynolds's system or is related to proper licensing. Authenticom denies the remaining allegations of Paragraph 4.

5. While the Reynolds DMS has a great deal of native functionality for core dealership functions like vehicle sales, financing and insurance, and inventory management, dealers can choose to use certain third-party software applications that supplement or replace the DMS's native functionalities. Just as some smartphone users prefer to install Google Chrome on their iPhones instead of using the native Safari browser, some dealers might prefer a third party's contact management application to the Reynolds DMS's native program. Dealers regularly assess the availability and compatibility of their preferred third-party applications when choosing a DMS platform. Accordingly, beginning in the early 2000s, Reynolds built a specialized functionality—today known as the Reynolds Certified Interface, or RCI, program—that enables third-party applications to function seamlessly with the Reynolds DMS. When an application vendor is approved to join the RCI program, Reynolds builds them customized software interfaces that allow the DMS and the application to communicate and exchange data in a secure and efficient manner. Dealers choosing a Reynolds DMS can easily determine if a particular third-party vendor is an available Reynolds RCI partner before making their DMS choice.

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 5 of the Counterclaims that relate to the details of Reynolds DMS, RCI program, or "customized" software interfaces, and on that basis denies them. Authenticom admits that some smartphone users prefer to install Google Chrome on their iPhones

instead of using the native Safari browser. Authenticom admits that some dealers prefer a third party's CRM application to the Reynolds DMS's native program. Authenticom denies the remaining allegations of Paragraph 5.

6. Each RCI interface package for each Reynolds RCI partner is precisely tailored to the corresponding application's needs, including the communication protocols, business rules, data elements, and the regularity of updates (such as integrated real-time and bi-directional capabilities, where necessary). Some application vendors purchase packages of ten or more interfaces, with each interface providing different functionalities and configured sets of data elements. The interfaces also run through a centralized hub, known as the Reynolds Integration Hub (RIH), which allows each data feed to be monitored, recorded, and supported with the requisite computing resources. Each certified vendor also signs a contract, known as a Reynolds Interface Agreement (RIA) that, among other things, contains a robust set of security requirements.

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 6 of the Counterclaims that relate to the RCI program, RIH, and details of the packages purchased by "some" vendors that Reynolds refers to, and on that basis denies them. Authenticom admits that vendors in the RCI program sign RIA agreements. Authenticom denies the remaining allegations of Paragraph 6 of the Counterclaims.

7. Reynolds charges (and has a right to charge) application vendors premium prices for its RCI interfaces. These prices recognize the tremendous value of the RCI interfaces—and packages of interfaces—as well as Reynolds's huge investments in building and maintaining those interfaces (as well as the rest of the Reynolds DMS). In this sense, Reynolds is no different from other computer system developers and operators that have spent years and millions of dollars to build secure access points and who, as a result of their investments in intellectual property, are free both to charge for their systems and to refuse access to those who decline to pay for the license to use the system or who threaten its integrity and security.

ANSWER: Authenticom admits that Reynolds charges supracompetitive prices for its RCI interfaces, but denies that they have the right to charge those prices or that they recognize any value of or investment in the interfaces. Authenticom denies the remaining allegations of Paragraph 7.

8. Counterdefendant Authenticom, Inc. is aware of the contractual and license restrictions on access to the Reynolds DMS. Nonetheless, Authenticom's business model for Reynolds DMS customers is based on stolen access to the Reynolds system. On a daily basis,

Authenticom tortiously interferes with Reynolds's contracts by inducing dealers to hand secure logins to Reynolds's system over to Authenticom, in what Authenticom knows is a breach of the dealers' license agreements with Reynolds. As explained herein, Authenticom then uses these misappropriated user IDs and passwords to run, log into, and use the Reynolds DMS, thereby fraudulently misrepresenting that it is an authorized dealership employee, bypassing critical access controls, and infringing Reynolds's copyrights. Authenticom next evades Reynolds's CAPTCHA and other access controls by, among other things, running a series of deceptive automated scripts that trick the system into believing that Authenticom is a bona fide—human—employee user in order to operate the DMS program and evade Reynolds's security measures. Authenticom then uses its automated software programs to activate the Reynolds system's robust reporting tools and other functionalities to Hoover up information through screen-scraping and high-volume automated downloads of data.

ANSWER: Paragraph 8 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom admits that dealers authorize Authenticom to retrieve their data, and at one time provided Authenticom with dealer-created login credentials to do so. Authenticom denies the remaining allegations of Paragraph 8.

9. Its electronic burglary having been accomplished, Authenticom then absconds with that information (much of it critically sensitive, none of it belonging to Authenticom) by exporting it to itself. With no evident sense of irony, Authenticom then sells the data and information it has obtained to third-party application vendors, who must agree to Authenticom's own licensing requirements but who—like Authenticom itself—have no license or right to use Reynolds's system in this manner.

ANSWER: Paragraph 9 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the allegations in Paragraph 9.

10. Authenticom's business model for Reynolds's systems rests on an ongoing, intentional, and staggering level of computer fraud and theft from Reynolds. Authenticom's thievery is calculated and intentional: it admits in its pleadings that it has worked with Reynolds's licensed dealers to develop "workaround solutions that circumvented Reynolds's efforts to block access to the Reynolds system." Reynolds put Authenticom on notice that its actions were illegal and unauthorized and demanded that it cease and desist, but to no avail. Authenticom has now repackaged itself as the victim of anticompetitive restrictions, bringing a suit the premise of which is that Authenticom has been deprived of the ability to engage in free, uncontrolled, and unlimited access to the Reynolds system for its own profit. Authenticom further touts its own prices as being the correct competitive benchmark—despite the fact that it can charge such prices only by freeloading on Reynolds's system's functionalities and intellectual property. But nothing in the law permits Authenticom to access the Reynolds DMS without permission from Reynolds, the

creator, owner, operator, and licensor of the DMS. Nothing in the law requires Reynolds to deal with Authenticom, either. Authenticom is a hacker, one that disguises its thievery in a cleverly pleaded euphemism, claiming it is in the business of providing “data integration”¹ services. Authenticom’s real business is system bootlegging: unlawfully logging into the Reynolds DMS, utilizing the system’s capabilities to process and report information, and then extracting, repackaging, and selling that information to others.

ANSWER: Paragraph 10 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the allegations in Paragraph 10.

11. In short, Authenticom’s Reynolds-DMS business model relies entirely on unauthorized, unsecure, and illegal access to a proprietary computer system that Reynolds has painstakingly built and protected at extraordinary expense. Authenticom is a software pirate that free-rides on a computer system it has not borne the cost of building, securing, or maintaining. And Reynolds, not Authenticom, will be left holding the bag if and when Authenticom’s uncontrolled, unmonitored, and unauthorized access methods and sloppy security practices cause a DMS system crash, data breach, or loss of intellectual property.

ANSWER: Paragraph 11 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the allegations in Paragraph 11.

12. Every time Authenticom provides its bootleg “integration” services to a dealer who licenses the Reynolds DMS software, it tortiously interferes with Reynolds’s contractual relationship with that dealer. Every time Authenticom uses misappropriated login credentials to access the Reynolds DMS without Reynolds’s authorization, it fraudulently misrepresents that it is an authorized dealership employee, commits a trespass to chattels under the common law, and violates the federal Computer Fraud and Abuse Act, the Wisconsin Computer Crimes Act, and the California Comprehensive Computer Data Access and Fraud Act. Every time Authenticom runs the Reynolds DMS PC software, it infringes Reynolds’s copyrights. Every time Authenticom circumvents Reynolds’s security measures that govern access to and copying of material on the DMS, it violates the Digital Millennium Copyright Act. Every time Authenticom succeeds in its unrelenting efforts to command Reynolds DMS servers to run and execute commands at Authenticom’s direction, Authenticom has converted those servers. Every time Authenticom accepts payment for its bootleg integration services, it unjustly enriches itself at Reynolds’s expense. In short, as it pertains to Authenticom’s unauthorized use of the Reynolds DMS system, its business is wholly unlawful. As a result, Authenticom’s business model violates the California Unfair Competition Law. Reynolds is entitled to a permanent injunction to compel Authenticom

¹ Authenticom calls itself a “dealer data integration provider,” but it admits it offers “no *actual* ‘integration’” services “in the traditional sense”; “[i]nstead, in this context, ‘integration’ is *simply a synonym for data access*.” Authenticom Dkt. 4 at ¶¶ 2, 54 n.4 (emphases added).

to stop.

ANSWER: Paragraph 12 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the allegations in Paragraph 12.

13. As a result of its wrongful and illegal actions, Authenticom is liable to pay statutory and common law damages to Reynolds. Reynolds is also entitled to additional equitable relief from Authenticom in the form of restitution and disgorgement of Authenticom's profits that relied, even in part, on unauthorized and stolen access to the Reynolds systems. Finally, Reynolds is entitled to a permanent injunction barring Authenticom from accessing the Reynolds system without Reynolds's authorization. Paying damages for past injuries, alone, is not enough: Authenticom has alleged its business model depends on its ability to use Reynolds's systems, despite its lack of a license to do so, and so it is overwhelmingly likely that Authenticom will continue to hack the Reynolds system in the future. Without injunctive relief, Reynolds will be forced into endless litigation, suing Authenticom over and over to recover damages for its future tortious conduct. That multiplicity of suits is itself a form of irreparable harm.

ANSWER: Paragraph 13 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the allegations in Paragraph 13.

I. PARTIES

14. Counterplaintiff The Reynolds and Reynolds Company is a privately held Ohio corporation with its corporate headquarters and principal place of business at One Reynolds Way, Kettering, Ohio 45430.

ANSWER: Admitted.

15. As alleged in its complaint, Counterdefendant Authenticom, Inc. is a privately held Wisconsin corporation with its corporate headquarters and principal place of business at 400 Main Street, La Crosse, Wisconsin 54601. *Authenticom* Dkt. 4 at ¶ 19.²

ANSWER: Admitted.

II. NATURE OF THE COUNTERCLAIMS

16. These counterclaims arise under the Computer Fraud and Abuse Act ("CFAA"), 18

² Throughout this complaint, references to the *Authenticom* docket are to the pre-consolidation docket in this case, 3:17-cv-00318-jdp, accessible via the Western District of Wisconsin PACER site.

U.S.C. § 1030; the Copyright Act, 17 U.S.C. § 501; the Digital Millennium Copyright Act (“DMCA”), 17 U.S.C. § 1201; the Wisconsin Computer Crimes Act (“WCCA”), Wis. Stat. § 943.70(2)(a); the California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502; the California Unfair Competition Law, Cal. Bus. and Prof. Code § 17200; and the common law.

ANSWER: The allegations in Paragraph 16 of the Counterclaims state legal conclusions to which no response is required. Defendant’s common-law conversion claim was dismissed under Federal Rule of Civil Procedure 12(b)(6); accordingly, no response is required as to that claim. Dkt. 506.

17. This Court has jurisdiction over these counterclaims pursuant to 28 U.S.C. §§ 1331, 1332(a)(1), 1367(a), 2201(a), and 2202. There is federal question jurisdiction under 28 U.S.C. § 1331 because Reynolds seeks to enforce its federal statutory rights under the CFAA, the Copyright Act, and the DMCA. There is diversity jurisdiction under 28 U.S.C. § 1332(a)(1) because Reynolds is a citizen of Ohio, Authenticom is a citizen of Wisconsin, and the amount in controversy with respect to these counterclaims exceeds the sum or value of \$75,000, exclusive of interest and costs. There also is supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367(a) because they are so related to claims in the action within the Court’s original jurisdiction that they form part of the same case or controversy under Article III of the United States Constitution.

ANSWER: Authenticom admits that Reynolds is a citizen of Ohio and that Authenticom is a citizen of Wisconsin. Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 17 of the Counterclaims that relate to the amount in controversy with respect to the counterclaims and on that basis denies them. The remaining allegations in Paragraph 17 state legal conclusions to which no response is required.

18. This Court has personal jurisdiction over Authenticom because it is located and does business in the District in which this action was filed; because many of its illegal actions challenged in these counterclaims occurred in, and/or were directed from, that District; and because Authenticom filed a complaint against Reynolds in that District.

ANSWER: The allegations in Paragraph 18 of the Counterclaims state legal conclusions to which no response is required. To the extent “that District” refers to the Northern District of Illinois, Authenticom denies that it filed its complaint against Reynolds in the Northern District of

Illinois; on the contrary, Authenticom filed its complaint in the Western District of Wisconsin and any trial in this matter will take place in the Western District of Wisconsin. Authenticom likewise denies that “many of the actions” giving rise to Reynolds’s counterclaims were “directed from” the Northern District of Illinois.

19. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(b) and (c).

ANSWER: The allegations in Paragraph 19 of the Counterclaims state legal conclusions to which no response is required.

III. RELEVANT BACKGROUND

a. The Reynolds DMS Is A Complex, Bespoke, Premium Computer System That Contains Highly Sensitive Data and Is Protected by Copyright

i. Reynolds Has Invested Hundreds of Millions of Dollars and Millions of Man-hours to Build the Most Stable, Secure, and Sophisticated Dealer Management System on the Market.

20. Reynolds was founded in 1866 and formally incorporated in Ohio in 1889. It has been partnering with retail automotive dealers to improve their business operations since the 1920s, when Reynolds created the first standardized account forms and a paper-based accounting system for the retail automotive industry.

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 20, and on that basis denies them.

21. Reynolds introduced “ERA,” the first computerized DMS, in the late 1980s. The Reynolds DMS is an integrated, complex system of hardware and software components that enable retail automotive dealers to manage their inventories, customer contacts, financial and insurance information, transactional details, government reporting and compliance requirements, human resources files, and a myriad of other tasks involved in managing an auto dealership. ERA is Reynolds’s principal DMS product.

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 21 of the Counterclaims that relate to the date of the release of the first computerized DMS and Reynolds’s claim that ERA was the first of these, and on that basis denies them. Authenticom admits that Reynolds has a DMS product called ERA.

Authenticom denies the remaining allegations of Paragraph 21 of the Counterclaims.

22. In October 2006, following a merger by acquisition, Reynolds and Dealer Computer Services, Inc. (“DCS”) merged operations. DCS had developed a separate DMS product in the 1980s. That product is currently known as POWER and continues to be offered under Reynolds’s ownership and control. Unless otherwise noted, ERA and POWER will collectively be referred to as “the Reynolds DMS.”

ANSWER: Authenticom admits that October 2006, Reynolds and DCS combined to form Reynolds. Authenticom admits that DCS developed a DMS product that is currently known as POWER, which is owned and controlled by Reynolds.

23. The Reynolds DMS consists of numerous hardware and software elements. At a very high level, those components include the following:

- a. A dealer-side server (either in the form of a standalone server physically on site at the dealership or a cloud-hosted server);
- b. An operating system on the server;
- c. Multiple databases on the server;
- d. Application software on the server;
- e. A secured software interface between the server and the dealer’s PCs;
- f. Terminal and application software on the dealer’s PCs;
- g. Secure data connections between the dealer-side server and the “Reynolds Integration Hub,” and
- h. The Reynolds Integration Hub itself, which includes numerous layers of security, monitoring and other proprietary functions designed to, among other things, seamlessly integrate numerous vendors, manufacturers, and others into the DMS ecosystem in a secure, real-time manner.

ANSWER: Authenticom admits that Reynolds has a DMS and that it has hardware and software elements, including database on which dealers store their data. Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in the remainder of Paragraph 23, and on that basis denies them.

24. The proprietary design and interaction of these various components reflects Reynolds's decades-long efforts to provide the most stable and secure DMS platform on the market. Reynolds has staked its brand and reputation on providing such a platform, and has invested heavily in building, securing, and maintaining its DMS platform. Over the course of the last two decades, those investments are easily in excess of hundreds of millions of dollars and millions of man-hours.

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 24, and on that basis denies them.

ii. The Reynolds DMS Does Not Merely Contain “Dealer Data”

25. Authenticom's core thesis in this litigation is that the data on the DMS “belongs to the dealer.” As an initial matter, that claim is a fundamental misdirect: the core dispute in this case is about *system* access, not *data* access—as evidenced by the fact that dealers have the ability to export their data from the DMS at will, using a robust and integrated suite of reporting tools (discussed below). Moreover, Authenticom's claim that the data on the DMS “belongs to the dealer” is also materially false. In addition to its many other functions and operations, Reynolds's proprietary system processes and stores not only dealer operational and financial data, but also confidential consumer, automotive original equipment manufacturer, financial institution, and credit bureau information, reference data, and intellectual property owned by Reynolds and other third parties. DMS-processed data includes numerous categories of sensitive “Personally Identifiable Information” or “PII.”

ANSWER: Authenticom admits that the data on the DMS belongs to the dealer. Authenticom admits that some of that dealer data includes transactional and customer information. The remainder of Paragraph 25 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 25.

26. Reynolds's DMS also processes a related, overlapping category of protected information known as Nonpublic Personal Information (“NPI”). Virtually all of the information that a consumer provides to a dealership constitutes either PII or NPI.

ANSWER: Authenticom admits that consumers provide some PII and NPI information to dealerships. Authenticom denies the remaining allegations in Paragraph 26.

27. In addition, Reynolds's DMS processes and securely stores sensitive information belonging to automotive manufacturers (“OEMs”), such as codes and prices for parts and labor, rebates and incentive information, and warranty information.

ANSWER: Denied.

28. Reynolds's DMS also processes and securely stores sensitive information belonging to other third parties, such as credit check information generated by Experian and other credit reporting bureaus.

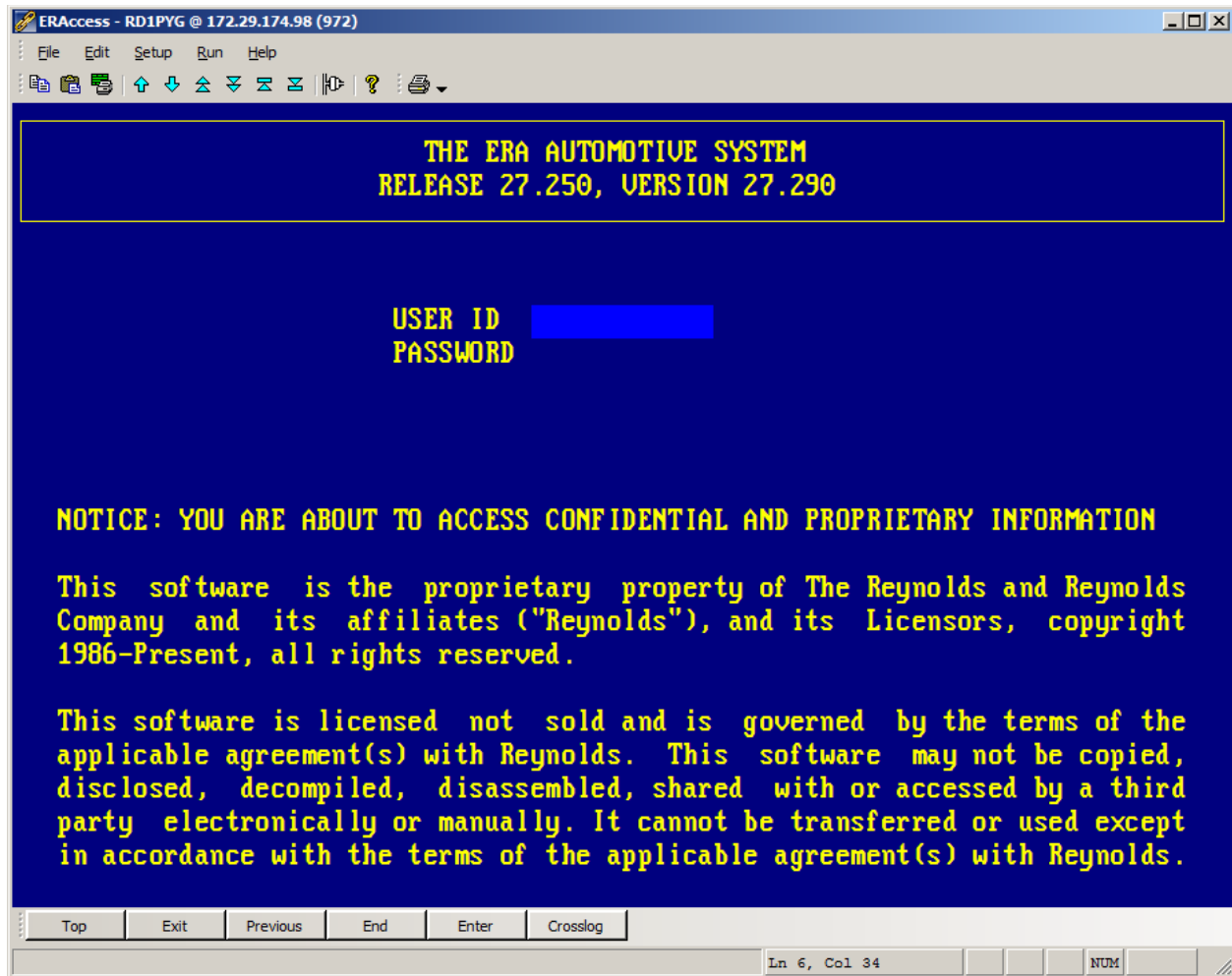
ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 28, and on that basis denies them.

29. In addition, Reynolds's DMS processes, and is largely comprised of, valuable intellectual property. This intellectual property includes, but is not limited to, the software that comprises the DMS itself.

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 29 of the Counterclaims related to what Reynolds's intellectual property holdings include, and on that basis denies them. Authenticom denies the remaining allegations in Paragraph 29 of the Counterclaims.

iii. Reynolds's DMS Is Protected by Copyright

30. The Reynolds DMS PC software program that runs on dealer computers is an original copyrighted work. Among the many significant original elements of the program are its source and object code; distinctive screen layouts; graphical content; text; arrangement, organization, and display of information; and dynamic user experience. Every time a user opens the DMS PC software program, the program displays a notice that, among other things, clearly and explicitly states that the program is Reynolds's copyrighted, confidential, and proprietary property:



ANSWER: Paragraph 30 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 30, and on that basis denies them.

31. As set forth below, it is impossible for a user to access or use the core DMS without running (and thereby copying) Reynolds's copyrighted DMS PC software programs.

ANSWER: Paragraph 31 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 31, and on that basis denies them.

32. Authenticom does not now have, nor has it ever had, Reynolds's permission to access or use the DMS to exfiltrate data and sell that data to third parties. Nor has it ever had a valid license or sublicense to do so.

ANSWER: Denied.

b. Reynolds Invested Heavily in the Reynolds Certified Interface Program to Build a Stable, Secure, Real-Time Data Transfer Platform.

33. As discussed above, Reynolds has staked its brand and reputation on providing the most stable and secure DMS platform on the market. Access to the DMS without Reynolds's authorization, especially automated access, constitutes a threat to that reputation, to the system, to Reynolds's intellectual property, and to the data stored on the system.

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 33 regarding what Reynolds has done and why it has done it, and on that basis denies them. Authenticom denies the remaining allegations in Paragraph 33 of the Counterclaims.

34. At the same time, Reynolds's dealership customers often desire to use various third-party applications as part of their business operations. These include software applications that provide automated license-plate registration, customer relationship management, dealership marketing assistance, information technology, website management, and other services. Other vendors, like TRUECAR, provide vehicle pricing for the dealers' customers using Vehicle Sold information from the dealers' inventories. Such third-party applications often desire to leverage the functionality and contents of the DMS platform.

ANSWER: Authenticom admits that Reynolds's dealership customers often desire to use third-party application providers for the various services listed, including those applications not owned by Reynolds. Authenticom denies the remaining allegations in Paragraph 34 of the Counterclaims.

35. Although many vendors wish to leverage the DMS by pulling processed data out of the DMS platform, some also seek the ability to "push" or "publish" data back into the DMS so that it can populate the DMS's various systems and databases for computation and organization by the system. For example, vendors seeking to amend customer records or input service appointments often desire such write-back abilities to allow that information to interact with the Reynolds systems' other functions.

ANSWER: Authenticom admits that some vendors desire to "push" data back into the DMS,

including vendors seeking to amend customer records or input service. Authenticom denies the remaining allegations in Paragraph 35 of the Counterclaims.

36. Providing dealers with a managed, functional, and secure method for applications to leverage the functionality and contents of the DMS is a critical part of ensuring that Reynolds's DMS is competitive in the DMS marketplace. Dealers are fully aware of what applications are licensed or authorized to leverage each DMS platform, and DMS providers frequently use applications' compatibility with their system as a point of competition with each other. Reynolds's RCI functionality is accordingly central to Reynolds's business strategy, distribution scheme, and marketing plan.

ANSWER: Authenticom admits that Reynolds competes in the DMS market and that it provides data access through the RCI program. However, Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 36 of the Counterclaims related to Reynolds's strategies, schemes, or plans, and on that basis denies them. Authenticom denies the remaining allegations in Paragraph 36 of the Counterclaims.

37. In order to facilitate secure real-time interfaces between the DMS and third-party applications, Reynolds developed technology to support the RCI program. The RCI program facilitates third-party interfaces that allow third parties to leverage the benefits of the DMS while imposing carefully constructed layers of safeguards and protections between the vendors and the DMS itself. It provides application vendors with the ability to both receive and, if appropriate, push data into the DMS via dedicated, customized interfaces. These interfaces are designed to ensure that a vendor receives only what is necessary for the dealer's business needs for that vendor and to minimize the impact of the additional DMS system burden. Reynolds's interface protocols ensure that third parties do not directly access the DMS.

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 37 of the Counterclaims related to Reynolds's motivations for developing its "technology," whether dealer's only receive what is necessary, or whether the RCI interface minimizes any impact on the DMS system, and on that basis denies them. Authenticom denies the remaining allegations in Paragraph 37 of the Counterclaims.

38. As part of its system, Reynolds has built over 1,600 customized interfaces, deployed in over 50,000 custom packages that engage in approximately 260,000,000 data transactions a month. Reynolds employs more than 5,000 people and devotes enormous resources to building, maintaining, and monitoring the DMS and its incorporated interface protocols through

its integration hub.

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 38 of the Counterclaims, and on that basis denies them.

39. Reynolds works with each vendor seeking RCI certification to determine the precise types of interface functionality and data element needs that the vendor requires to operate its application, the specific business rules that will apply to the data, the frequency with which the data needs to be refreshed, and, as appropriate, whether the application needs bidirectional interface functionality. The interfaces are then built, configured, and tested to ensure that the third-party application is appropriately interfacing with the DMS.

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 39 of the Counterclaims, and on that basis denies them.

40. Reynolds has built numerous safeguards—including redundant layers of hardware and software protection—into the DMS to support system stability. For example, the RIH includes a “journaling” function that protects against the risks inherent in allowing large-scale automated “write-back” from vendor software into dealer databases. After vendor software performs its particular function, dealers and vendors want the results of that function to be reflected in the Reynolds DMS servers and populated according to the system’s proprietary business rules. To take a common example, a dealer using third-party inventory management software would typically want that software to be able to accurately update the number of cars on the lot following a sale. But large-scale automated write-backs, if permitted, come with inherent risk: these automatic data pushes involve far more entries and transactions than an individual human user could produce, and if the vendor software malfunctions, it can produce and push thousands of erroneous data entries in the span of minutes. Those erroneous data entries can have a contagion effect as they propagate across the dealer’s system—since many DMS functionalities rely on data streams from other portions of the DMS—potentially paralyzing the dealer’s operations.

ANSWER: Further, Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 40 of the Counterclaims related to what safeguards Reynolds has built, what the RIH includes and how it functions, and on that basis denies them.

Authenticom denies the remaining allegations in Paragraph 40 of the Counterclaims.

41. Reynolds’s journaling technology—which Reynolds built from the ground up—is a critical backstop that allows Reynolds to unwind the potentially catastrophic effects of malfunctioning vendor software. Journaling minimizes potential down time for dealers and vendors, as well as the risk of DMS data being erroneously overwritten by a vendor.

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the

truth of the allegations in Paragraph 41 of the Counterclaims related to whether Reynolds built its journaling technology, what it entails, how it did so, and on that basis denies them. Authenticom denies the remaining allegations in Paragraph 41 of the Counterclaims.

42. Reynolds's integration protocols, support and monitoring, and the RCI program further ensure that dealers' DMSs are not overloaded as a result of third parties "pinging" the system with constant computer processing requests. The dealer side of the DMS is never pinged or touched by RCI partners. RCI (via the RIH) provides Reynolds with the ability to monitor each vendor's data feed and promptly detect any disruptions or errors in real time. Reynolds's integration technology provides Reynolds with the ability to audit and trace potential security breaches. Reynolds integration technology also protects system stability because its custom interfaces are carefully designed to avoid disrupting critical system updates and tasks.

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 42 of the Counterclaims related to whether the dealer side of the DMS is ever pinged or touched by RCI partners or Reynolds' ability to monitor the RIH, and on that basis denies them. Authenticom denies the remaining allegations in Paragraph 42 of the Counterclaims.

43. In addition to its own proprietary system security measures, Reynolds also imposes stringent contractual security obligations on its RCI vendor partners in their license and interface agreement. RCI vendors are prohibited from using unapproved methods to access the DMS; are required to notify Reynolds promptly in the event of a security breach; and must warrant to Reynolds that they comply with data security and privacy laws. Moreover, Reynolds requires vendors to include certain terms in their End User License Agreements with dealers. One of these terms requires both the vendor and dealer to implement and maintain safeguards designed to protect sensitive customer information. Reynolds reserves the right to—and frequently does—audit its RCI vendor partners' End User License Agreements to ensure compliance. These contractual requirements for RCI certification protect dealer and consumer data by aligning incentives, and they also give Reynolds an avenue for indemnification in the unlikely event that an RCI partner suffers a data breach.

ANSWER: Authenticom admits that Reynolds imposes stringent contractual obligations on RCI vendor partners, but denies that Reynolds is motivated by security and denies that the contractual requirements described protect data or align incentives. Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 43 of the

Counterclaims related to whether Reynolds reserves the right to or ever does perform audits of license agreements, and on that basis denies them. Authenticom denies the remaining allegations in Paragraph 43 of the Counterclaims.

44. Of course, when Authenticom uses automated software to access, use, and scrape data from the DMS, and then sends that data to unknown and unapproved third parties, Reynolds receives no such assurances. Hostile data scrapers like Authenticom that mask as credentialed dealer-side employee users also bypass *all* of these important safeguards and rob dealers of the system stability and protection they bargained for with a Reynolds DMS.

ANSWER: Denied.

45. These mission-critical security and stability measures—customized interfaces with carefully limited data access, multilayered hardware and software redundancies, sophisticated journaling, and segregation of vendor system interaction from dealer-side communication with the Reynolds DMS servers—were expensive and difficult to build, and are expensive and difficult to maintain. Just as the Reynolds system is a premium DMS, the RCI program is a premium integration platform. It provides best-in-class stability and security.

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 45 of the Counterclaims related to the costs of building or maintaining Reynolds's DMS servers, and on that basis denies them. Authenticom denies the remaining allegations in Paragraph 45 of the Counterclaims.

c. Reynolds Provides Dealers with Robust Tools to Export Their Data from the DMS.

46. Although automated access is not allowed by either the Reynolds system or the license agreements under which it is offered, Dealers are authorized and able to use the robust reporting functionality built into the system to export operational data as needed. [REDACTED]

ANSWER: Denied.

47. Reynolds's ERA DMS contains a functionality called Dynamic Reporting. This reporting tool allows dealership employees to build customized reports—i.e., data exports from the DMS—with extensive flexibility. Dynamic Reporting reports can be scheduled to run at any time automatically, up to four times a day. They can also be run manually by a dealership employee at any time. Dealers can then send or push to the third party, or allow the third party access to a

PC where the downloaded data is housed. (POWER contains analogous features, although there are some technical differences.) Previous versions of the Reynolds DMS also contained similar (though less advanced) reporting tools called Report Generator and Query Builder.

ANSWER: Authenticom admits that Reynolds’s ERA DMS has a reporting tool called Dynamic Reporting, but denies that it is “customized” or that it has “extensive flexibility.” Authenticom admits that Dynamic Reporting reports can be run manually and that dealers can transmit that data to third parties, including by allowing a third party access to a PC where the downloaded data is housed. Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the remaining allegations in Paragraph 47 of the Counterclaims, and on that basis denies them. Authenticom denies the remaining allegations in Paragraph 47 of the Counterclaims.

48. In addition, Reynolds offers a program called AVID—“Automated Vehicle Inventory Downloads”—by which Reynolds has configured an automated report for third parties to retrieve vehicle-inventory data. The AVID process pushes the vehicle-inventory data to a secure destination (at the dealership or to Reynolds), where dealers can arrange for third parties to retrieve it. In addition, Reynolds provides dealers with several data transfer options related to their banking and payroll functions, including positive pay and direct deposit.

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 48, and on that basis denies them.

49. Reynolds’s clearly articulated and widely publicized policy for *over a decade* has been that, outside of the options noted above, “all third-party vendors that want data from a dealership’s Reynolds system [must] be certified through the Reynolds Certified Interface program or receive the data via a download from Dynamic Reporting.” *Authenticom* Dkt. 71-8 (Nemelka Decl. Ex. 33). Reynolds has not been secretive about these policies, but rather has been the industry leader in requiring certified interfaces with its system as “the safest way to protect [dealer] data ... while still supporting the need for moving data to third parties and OEMs.” *Authenticom* Dkt. 71-7 (Nemelka Decl. Ex. 32); *see also Authenticom* Dkt. 70-21 (Nemelka Decl. Ex. 21). Reynolds maintains that utilizing certified interfaces is the best way to transfer data—particularly of a sensitive nature—but at the end of the day, Reynolds’s dealership customers are free to take all of their operational data out of the DMS and send it to Authenticom (or others) whenever they want, subject only to their own independent legal, regulatory, and ethical obligations.

ANSWER: Authenticom admits that the quoted text appears in the declaration exhibits cited, but denies Reynolds's accuracy in its use of the quotations. Beyond that, Paragraph 49 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 49 of the Counterclaims.

d. Reynolds Has Secured its DMS System with a Series of Safeguards Designed to Thwart Unauthorized Access, Use, and Copying.

50. Because the Reynolds DMS is critical to business operations and includes commercially valuable intellectual property and critically sensitive data belonging to Reynolds, automobile manufacturers, dealers, and dealership customers, Reynolds carefully controls access to the DMS platform to maintain robust system stability and functionality, prevent unauthorized use, and guard data security.

ANSWER: Authenticom admits that the DMS contains data that belongs to dealers. Beyond that, Paragraph 50 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 50 of the Counterclaims.

51. Access to the DMS by a dealership is controlled through a series of security measures, beginning with a login prompt that requires a user to enter a valid username and password to use the system. After a user has successfully logged in, the user encounters a series of visible and invisible security measures in the course of accessing and using different parts of the Reynolds DMS.

ANSWER: Authenticom admits that there is a login prompt in connection with the Reynolds DMS. Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 51 of the Counterclaims related to the "visible and invisible" measures, and on that basis denies them. Authenticom denies the remaining allegations in Paragraph 51 of the Counterclaims.

52. For example, users who want to use the DMS's data exporting functions must pass through a CAPTCHA control. The test consists of a word or series of letters and numbers that have been stretched and twisted, typically displayed against a color-gradient background. Because

humans and computers process and recognize patterns differently, humans can easily pass CAPTCHA controls, whereas bots and similar automated scripts encounter difficulties. It is impossible for a dealer user to access these and other portions of the Reynolds DMS platform without passing a CAPTCHA control.

ANSWER: Authenticom admits that Reynolds has inserted CAPTCHA prompts. Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 52 of the Counterclaims related to the possibility of access to portions of the DMS without encountering CAPTCHA, and on that basis denies them. Beyond that, Paragraph 52 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 52 of the Counterclaims.

53. A suite of invisible access controls also helps secure the Reynolds DMS from would-be hackers. For example, Reynolds's Suspicious User ID monitoring software monitors a variety of factors that differentiate automated scripts and bots from bona fide human users, including but not limited to keystroke speed, keystroke pattern, and the volume and timing of data requests. When the software determines that users are suspicious, based on a combination of the factors it monitors, the system protocols flag that user ID for deactivation. These system controls are agnostic as to the identity of the would-be hacker and are automatic.

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 53 of the Counterclaims related to the functionality of Reynolds's ID monitoring software, and on that basis denies them. Authenticom denies the remaining allegations in Paragraph 53 of the Counterclaims.


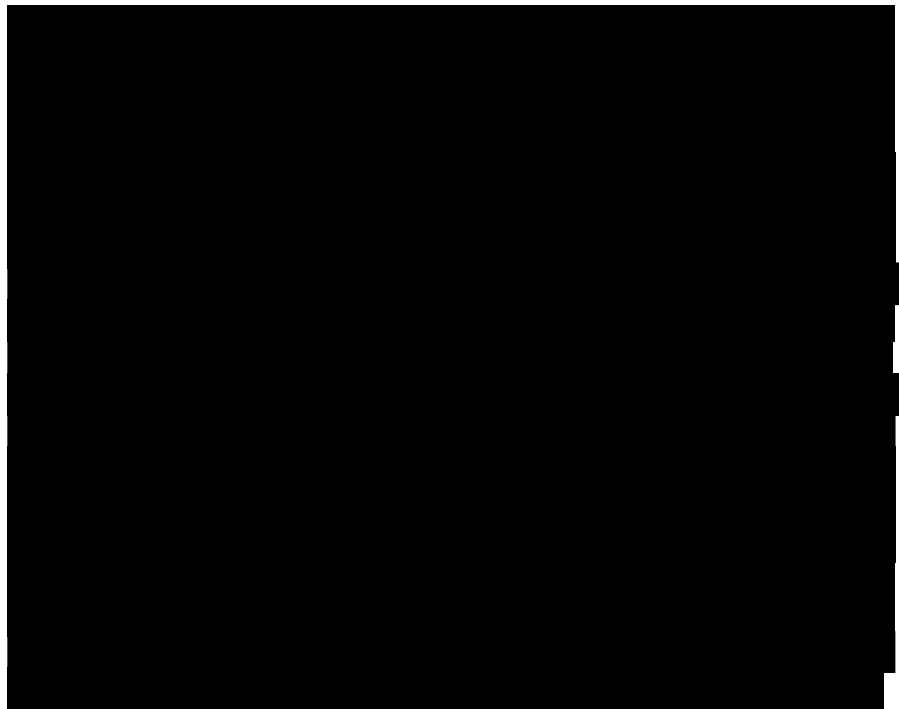

e. Reynolds's Licensing Agreements Explicitly Prohibit Dealers from Allowing Third Parties Like Authenticom to Access and Use the DMS System.

54. Reynolds licenses its DMS to dealerships pursuant to the Reynolds Customer Agreement, which is a licensing agreement that grants [REDACTED]

ANSWER: Authenticom admits that the quoted text appears in the cited declaration, and that

Reynolds's contracting practices subject dealers to numerous, anticompetitive conditions and restrictions. Beyond that, Paragraph 54 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 54 of the Counterclaims.

55. Authenticom has admitted in its own proposed findings of fact at the preliminary injunction hearing that Reynolds's contracts categorically prohibit dealers from giving access to the DMS to "any third party." *Authenticom* Dkt. 63 at ¶ 153; *see also Authenticom* Dkt. 65-24 § 1 (Nemelka Decl. Ex. 49).



ANSWER: Authenticom admits that the quoted text appears in the cited documents (with alterations), but denies the Reynolds is accurately characterizing the quoted text in Paragraph 55 of the Counterclaims. Beyond that, Paragraph 55 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies

the remaining allegations in Paragraph 55 of the Counterclaims.

56. [REDACTED]

ANSWER: Authenticom admits that the quoted text appears in the cited documents, but denies that Reynolds is accurately characterizing the contract language in Paragraph 56 of the Counterclaims. Beyond that, Paragraph 56 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 56 of the Counterclaims.

57. [REDACTED]

ANSWER: Authenticom admits that the quoted text appears in the cited document. Beyond that, Paragraph 57 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 57 of the Counterclaims.

58. [REDACTED]

ANSWER: Authenticom admits that the quoted text appears in the cited documents, but denies that Reynolds is accurately characterizing the contract language in Paragraph 58 of the Counterclaims. Beyond that, Paragraph 58 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 58 of the Counterclaims.

59. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

ANSWER: Authenticom admits that the quoted text appears in the cited documents (with alterations), but denies that Reynolds is accurately characterizing the contract language in Paragraph 59 of the Counterclaims.

60. [REDACTED]

[REDACTED]

ANSWER: Authenticom admits that the quoted text appears in the cited documents (with alterations), but denies that Reynolds is accurately characterizing the contract language in Paragraph 60 of the Counterclaims.

61. Authenticom is, and at all times relevant to the claims at issue in this suit has been, aware of these restrictions. The fact that Reynolds imposes these contractual licensing restrictions has been widely known in the automotive industry for more than a decade, as has the fact that Reynolds actively enforces the restrictions, both legally and technologically. Authenticom's own

complaint cites *Automotive News* articles proclaiming these policies in 2006-2008.

ANSWER: Denied.

62. In 2013, the United States District Court for the Southern District of Ohio further recognized Reynolds's licensing restrictions in dismissing another putative integrator's antitrust claims against Reynolds in a public order, stating:

Reynolds' auto-dealership customers agree to certain prohibitions on integration of third party applications when the customers license Reynolds' ERA. When they sign up for ERA, customers typically agree to prohibitions on connecting third-party applications to ERA. The customers also agree to prohibitions on allowing third-party integrators that are not licensed by Reynolds, like SIS, to interface with ERA.

Reynolds & Reynolds Co. v. Superior Integrated Sols., Inc., 1:12-CV-848, 2013 WL 2456093, at *2 (S.D. Ohio June 6, 2013) (citations omitted).

ANSWER: Authenticom admits that antitrust claims against Reynolds were dismissed in 2013, before Reynolds entered into a conspiracy with its chief competitor CDK. Beyond that, Paragraph 62 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 62 of the Counterclaims.

63. On the stand, Authenticom's founder and president, Stephen M. Cottrell attempted to equivocate on the issue of whether he was aware of the restrictions, stating that "there were lots of things that had been said" and "lots of talk in the marketplace" about the Reynolds license's controls on dealer's ability to allow third parties to access and use the Reynolds DMS. *Authenticom* Dkt. 162 (6/26/17 Afternoon Session Tr. at 19:11-16). But later, Authenticom produced documents clearly indicating that it was in fact provided copies of the specific language in Reynolds's licensing agreements prohibiting its access. To the extent there could have been any doubt about Reynolds's policy (there couldn't have been), Mr. Cottrell actually received a copy of the contractual restrictions in 2015 in connection with Reynolds's continued demands that Authenticom cease and desist from its illegal activity. Ultimately, Mr. Cottrell testified that he was aware of the exact language prohibiting dealers from giving Authenticom login credentials as of the first quarter of 2015. *Id.* at 18:17.

ANSWER: Authenticom denies the characterization of Mr. Cottrell's testimony and the documents Authenticom produced. Beyond that, Paragraph 63 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required,

Authenticom denies the remaining allegations in Paragraph 63 of the Counterclaims.

64. These licensing restrictions are a core aspect of Reynolds's business strategy, distribution scheme, and marketing plan. Reynolds is in the business of building and licensing a robust computer software and hardware ecosystem, and its controls on access to and use of that environment are absolutely central to its ability to control, operate, maintain, monitor, and secure its proprietary DMS platform.

ANSWER: Denied.

65. Some dealers disagree with these prohibitions on third party and automated access, while others appreciate and affirmatively agree with them. Dealers who disapprove of the restrictions are free to switch from Reynolds to other DMS providers that follow less stringent data security practices (or decline to use Reynolds in the first place) as a result of these contractual requirements. In fact, many dealers have switched to other DMS providers' more "open" systems. At the same time, numerous other dealers have either switched or returned to Reynolds because they prefer the stability, security, and other premium features that its DMS provides.

ANSWER: Authenticom admits that some dealers object to Reynolds's restrictive business practices, but denies that any dealers "appreciate" them. Authenticom admits that some dealers have switched from and to the Reynolds DMS. Beyond that, Paragraph 65 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 65 of the Counterclaims.

66. One of Authenticom's counsel's other clients in this MDL – Cox Automotive – specifically commissioned a study by "partner[ing] with two independent research firms to conduct studies with hundreds of dealer respondents." According to Cox's public statements about this report, at contract renewal 45% of small groups, 31% of medium sized groups, and 21% of large groups switched at their last renewal date. Switching is common. Dealers have a choice of DMS providers, and Reynolds offers a stable, robust option to sophisticated dealers that is premised, at its core, on a controlled computing environment.

ANSWER: Authenticom admits that its counsel has (a multitude) of other clients with claims against the anticompetitive business practices of Reynolds, and that Cox Automotive has made public statements about a study that it commissioned. Authenticom denies the remaining allegations in Paragraph 66 of the Counterclaims.

f. For Years, Authenticom Has Relentlessly Hacked the Reynolds DMS in Order to Sell Data to Unknown Third Parties, Placing Critically Sensitive Data at Risk and

Compromising System Functionality.

67. In order to facilitate its cut-rate bootlegging, Authenticom induces dealers to violate their Reynolds license agreements by sharing existing login credentials or creating new ones for Authenticom to use, then allowing Authenticom's hostile bots to access and use the system, as Mr. Cottrell testified at the preliminary injunction hearing. *Authenticom* Dkt. 164 (6/26/17 Morning Session Tr. 108:4-7). Authenticom then sells the fruits of this unauthorized hoovering to other outside parties.

ANSWER: Denied.

68. Reynolds has put Authenticom on notice that its "brazen" attempts to gain "unauthorized access" to Reynolds's DMS are "contrary to Reynolds's security policies, compromise[] the operational integrity of Reynolds's system and, perhaps most importantly, violate[] the agreements that Reynolds enters into with its dealership customers." *Authenticom* Dkt. 72-7 (Nemelka Decl. Ex. 57). For its part, following the Court's dismissal of its unsupportable exclusive dealing claim aimed at the Reynolds dealer licensing agreements, Authenticom elected not to challenge these agreements. In other words, the contractual restrictions on dealers sharing credentials to Reynolds's proprietary system are *not* challenged Reynolds conduct.

ANSWER: Authenticom admits that Reynold's selectively quoted text that appears in the cited document. Beyond that, Paragraph 68 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 68 of the Counterclaims.

69. Reynolds unequivocally has demanded that Authenticom "cease and desist from accessing Reynolds's proprietary software and hardware without the proper license and authorization to do so." *Id.* Authenticom admits, as it must, that Reynolds repeatedly has objected to Authenticom's actions as constituting tortious interference with Reynolds's dealer and vendor contracts. *See Authenticom* Dkt. 69 at ¶ 188-89.

ANSWER: Denied.

i Authenticom Knowingly Induces Dealers to Breach Their License Agreements by Providing Authenticom With Reynolds DMS Login Credentials

70. In its complaint, Authenticom admits that it repeatedly has used its improperly-obtained credentials to "bridge" into the Reynolds DMS without Reynolds's permission or authorization and, using "user emulation" software, "pull[ed]," "extract[ed]," and "scrape[d]" data from within the Reynolds DMS for sale to third-party vendors and "'push[ed]' data back into the DMS database" in altered form. *Authenticom* Dkt. 4 at ¶¶ 50, 54-55 & n.4, 77-80. Indeed, Mr. Cottrell has bragged that his company gives vendors a "pipeline into [Reynolds] dealerships." But this "pipeline" is really a series of brazen and illegal hacks. The centerpiece of Authenticom's

hacking efforts is an automated program that uses unauthorized and unlawful means to log into the proprietary Reynolds DMS, bypass or break through critical security and access controls, and execute Reynolds's proprietary, copyrighted software to suck data out of the DMS. *Authenticom* Dkt. 104-22 at 9 (Gulley Decl. Ex. 66). Through this chosen business model, Authenticom has trampled on Reynolds's contractual and intellectual property rights, trespassed on Reynolds's servers, created significant impairments and risks of harm to both Reynolds's DMS and its customers, and profited on the back of Reynolds's significant investment.

ANSWER: Denied.

ii. Authenticom Repeatedly And Persistently Circumvents Reynolds's DMS Access Controls

71. Reynolds has backed its objections up with continuing efforts to protect the DMS, including through continuous modifications and improvements to the security measures described above. Authenticom admits that, since at least 2009, Reynolds has been "disabling," "disrupting," and "blocking" Authenticom's unauthorized efforts to get inside Reynolds's DMS. *Authenticom* Dkt. 69 at ¶¶ 109-12, 137, 191. Indeed, according to Mr. Cottrell, Reynolds undertook "intensified" blocking efforts in 2013 that "resulted in an almost complete collapse of Authenticom's integration business for dealers using the Reynolds DMS." *Authenticom* Dkt. 62 at ¶ 38.

ANSWER: Reynolds selectively and misleadingly quotes from documents, and therefore the allegations in Paragraph 71 with respect to those documents are denied. Authenticom denies the remaining allegations in Paragraph 71 of the Counterclaims.

72. One auto industry analyst has likened the situation to a game of "Whack-A-Mole": "Vendors get shut out, and then find a way to work around the problem by finding a 'hostile' or backdoor entry. Reynolds then finds the backdoor entry and shuts it down." *Authenticom* Dkt. 71-14 (Nemelka Decl. Ex. 39). Every time Reynolds puts an access control in place, Authenticom attempts—sometimes successfully—to hack around the control.

ANSWER: Reynolds selectively and misleadingly quotes from documents, and therefore the allegations in Paragraph 72 with respect to those documents are denied. Authenticom denies the remaining allegations in Paragraph 72 of the Counterclaims.

73. 

ANSWER: Denied.

74. [REDACTED]

ANSWER: Reynolds selectively and misleadingly quotes from the documents cited, and therefore the allegations in Paragraph 74 with respect to those documents are denied. Authenticom denies the remaining allegations in Paragraph 74 of the Counterclaims.

75. [REDACTED]

ANSWER: Denied.

76. Similarly, Authenticom has consistently adapted its “user emulation” software to avoid Reynolds’s Suspicious User ID monitoring software. Reynolds does not know the details of how Authenticom has modified the program to avoid Suspicious User ID detection, but Authenticom has engaged in a persistent campaign to circumvent this protection measure since Reynolds first introduced it in 2013.

ANSWER: Denied.

77. Authenticom’s own complaint states that, in response to Reynolds’s longstanding efforts to prevent Authenticom and others from hacking into the Reynolds DMS, Authenticom has attempted for years to “navigate around” Reynolds’s “blocking efforts”—i.e., hack around the security measures discussed above, including login controls, CAPTCHAs, and the Suspicious User ID detection software—through various “workaround solutions,” including “user emulation” (i.e., falsely representing to be dealers logging into their own DMS accounts). Compl. ¶¶ 55, 195.

ANSWER: Denied.

78. According to its preliminary injunction briefing, Authenticom “worked with dealers to develop workaround solutions that circumvented Reynolds’[s] efforts to block access” to the Reynolds DMS. *Authenticom* Dkt. 67 at 8.

ANSWER: Authenticom admits that the selectively and misleadingly quoted text appears in

the cited document, but it denies Reynolds's characterization of that text.

79. Despite Reynolds's best efforts, Authenticom's circumvention efforts were often successful, and it repeatedly accessed the Reynolds DMS after disabling, bypassing, or evading the various security measures Reynolds had in place. The above citations to Authenticom's pleadings, briefing, documents, and testimony make clear that Authenticom circumvented Reynolds's access controls as a matter of routine. Authenticom's document production since then leaves no doubt: Authenticom's business model with respect to Reynolds was to hack around Reynolds system security.

ANSWER: Denied.

80. Authenticom even advertises its ability to circumvent Reynolds's access control measures, at one point publicly vowing to continue to hack its way into the DMS "*despite whatever hurdles are placed in our path.*"³ Authenticom has repeatedly emphasized its ability and intent to, in Mr. Cottrell's euphemistic phrasing, "navigate around the shutdowns." *Authenticom* Dkt. 62 at ¶¶ 40-41; *see also Authenticom* Dkt. 69 at ¶¶ 210-11.

ANSWER: Denied.

g. Authenticom Has Made Countless Copies of Reynolds's Copyrighted Software, Without Any Valid License or Sublicense

81. After bypassing the login and other access controls, Authenticom's bots run the Reynolds DMS PC software program using automated scripts that "emulate" a dealership employee's use of the system. *Id.* at 108:15-19. Every time Authenticom accesses and runs the Reynolds DMS PC software, it creates a copy of the copyrighted DMS PC software program code in the computer's Random Access Memory.

ANSWER: Denied.

82. 

ANSWER: Denied.

h. Authenticom's Actions Have Caused Extensive, Ongoing, and Irreparable Harm to

³ Stephen Cottrell, *Why Certification?* (Authenticom public letter dated June 2015), *available at* <https://web.archive.org/web/20160418122902/http://www.authenticom.com/pdf-downloads/Why%20Certification.pdf> (Wayback Machine internet archive snapshot from April 18, 2016, last visited February 20, 2018).

Reynolds, While Furthermore Imperiling Reynolds, Dealers, and Consumers

83. Authenticom's relentless efforts to hack into Reynolds's DMS and to "scrape" and "extract" information out of the Reynolds DMS without Reynolds's permission have caused a variety of serious and ongoing injuries to Reynolds and its dealers. In addition to the threat posed to the integrity and functionality of the Reynolds DMS itself, Authenticom has put at risk automotive manufacturers, credit bureaus, financial institutions, and, most importantly, millions of people whose PII and other confidential data are jeopardized by Authenticom's casual approach to cybersecurity.

ANSWER: Denied.

84. Hostile integrators like Authenticom are a cyber-security "black hole"—a catastrophic data breach just waiting to happen. Authenticom's hacking and unauthorized access practices violate widely accepted cybersecurity practices and directly contradict guidance from the National Automotive Dealers Association.

ANSWER: Denied.

85. Authenticom bypasses all of the interfaces, protections, and resources that Reynolds has built into its dedicated integration hub by accessing the system as a purported individual employee user with illegally obtained employee credentials. Authenticom instructs Reynolds's DMS licensees to configure access credentials for Authenticom's use with access set to "Grant Access to All Data Sets in All Run Areas" (the broadest DMS access setting for employee users) and then directly accesses the DMS through these pirated log-in credentials—as though it was an authorized dealership employee. This employee user-access setting enables a user to access substantially all of the data on the DMS available to the most-trusted dealership employee, regardless of the scope of work that Authenticom is meant to provide for the dealer or for the third-party software applications that are paying Authenticom. Given that configuration, Authenticom's assertion that it only accesses the narrow category of information that the vendor requires and the dealer authorizes is flatly untrue. And given the indiscriminate character of Authenticom's data collection techniques—screen scraping and bulk automated downloads—Authenticom's more limited assertion that it only *copies* the fields that vendors require and dealers authorize is almost certainly false.

ANSWER: Denied.

86. Moreover, although bootleggers like Authenticom seek to imitate real time access like that provided by RCI, they cannot do so. Genuine real-time access is available only from the system provider. (That's why application providers that want true real-time access pay an "open" system provider like Cox more for system integration (i.e., "OpenTrack"), even though Cox also authorizes non-integrated, third-party access like Authenticom's).

ANSWER: Denied.

87. Instead of the real-time data transfer that RCI offers, Authenticom accesses the

system from the *dealer side* (designed for and licensed for use by only human dealership employees) with thousands of automated transactions to scrape information, causing system load and harming stability and system performance. All the while, Authenticom bypasses the critical central safeguards of Reynolds's integration technology (which was designed and built precisely to securely and efficiently handle automated commercial integration for specific commercial users). Put simply, *any* unauthorized, uncontrolled access threatens the Reynolds DMS (as it would any computer system or network). Indeed, from Reynolds's perspective, Authenticom's access attempts and methods are indistinguishable from a hostile hacker. That is why Reynolds and other computer system operators go to extraordinary lengths to prophylactically detect and block unauthorized and uncontrolled access.

ANSWER: Denied.

88. Authenticom's position on cybersecurity appears to be: "Trust us." But Authenticom does not appear to be especially trustworthy when it comes to its data security practices. Authenticom's cavalier attitude toward cybersecurity is best summarized by reference to Mr. Cottrell's testimony at the preliminary injunction hearing.

ANSWER: Denied.

89. Cross-examination revealed that Mr. Cottrell falsely represented to the court that Authenticom had for three years received a Microsoft "gold security certification"—a certification that does not exist. *Compare Authenticom* Dkt. 62 at ¶ 31 *with Authenticom* Dkt. 162 (6/26/2017 Afternoon Session Tr. at 25:15-26:10). In any event, Microsoft itself is clear that simply being a customer of its Azure storage platform does not ensure Authenticom is secure or obviate Authenticom's many security obligations.⁴ Indeed, the highly publicized recent data breach at Deloitte occurred on the same Microsoft Azure platform that Authenticom has touted.⁵

ANSWER: Denied.

90. Cross-examination also suggests that, whatever the sincerity of Mr. Cottrell's professed passion for security, he is woefully uninformed about cybersecurity developments, not only in his own market segment but as regards his own data transfer partners. In August 2016, the cybersecurity press broke news that DealerBuilt—a competitor DMS—had suffered a serious data breach incident that resulted in millions of individuals' confidential information being leaked online. Dfts. P.I. Ex. 151.⁶ At the June 2017 hearing (over ten months later) Mr. Cottrell testified that he "just recently learned" of the DealerBuilt breach, *despite the fact that Authenticom has a data transfer agreement with DealerBuilt*. *Authenticom* Dkt. 162 (6/26/2017 Afternoon Session

⁴ See Frank Simorjay, *Shared Responsibilities for Cloud Computing* at 5 (Microsoft White Paper, April 2017), available at <https://perma.cc/3D2Q-TCPH>.

⁵ See, e.g., Nick Hopkins, *Deloitte hit by cyber-attack revealing clients' secret emails*, *The Guardian* (Sep. 25, 2017), available at <https://perma.cc/7PVL-3FS3>.

⁶ See also Zack Whittaker, *Bought a Car Recently? Millions of dealership customer details found online*, *ZDNet* (Nov. 8, 2016), available at <http://www.zdnet.com/article/bought-a-car-recently-millions-of-customers-records-found-online/> [<https://perma.cc/4K85-8GQN>]

Tr. at 22:1-6). This bears repeating: Authenticom's CEO and President was unaware, for nearly ten months, of a massive data breach that affected his own data transfer partner.

ANSWER: Denied.

91. Authenticom, itself, uses methods known to pose cybersecurity risks, including apparently using hardcoded credentials and poor security practices that allow plaintext credentials to its servers to be found on the Internet.

ANSWER: Denied.

92. Incredibly, Mr. Cottrell testified that, in his opinion, DMSs are "not a high value target" and so he did not think it was likely that hackers would target them. *Id.* at 23:2-5.

ANSWER: Denied.

93. This blasé attitude toward the security of the highly sensitive information stored on the DMS infects Authenticom's cybersecurity practices from root to branch. For example, Authenticom regularly communicates confidential DMS login credentials over the telephone and via unencrypted clear text in email or web forms. Per Authenticom's configuration instructions described above, these credentials—transmitted "in the clear"—have access to *substantially all of the information on the DMS* and are harvested by Authenticom *for the express purpose* of creating an outside "pipeline" to the DMS (in Mr. Cottrell's words). This is all before the information is stored by DealerVault (or Azure) and before it is sold and *retransferred* to other third parties (to possibly be re-retransferred by them).

ANSWER: Denied.

94. Moreover, based on information received in discovery and otherwise, it is apparent that Authenticom's network and infrastructure security is poor at best. Authenticom has already produced one report indicating that it was subject to a malware infection, and it is highly likely that discovery will expose other vulnerabilities and network breaches. These vulnerabilities would allow hackers to penetrate Authenticom's lackluster cybersecurity measures and access and copy the sensitive consumer, dealer, and institutional data that Authenticom purloined from the Reynolds DMS—as well as potentially Authenticom's pool of improperly-obtained Reynolds DMS credentials. In other words, after Authenticom hacks into and steals data from the Reynolds DMS, it stores that data in an unsecure location where it is vulnerable to be stolen once again by other, still less scrupulous hackers.

ANSWER: Denied.

95. Even if Authenticom was solid and reliable on data security (and it is not), the basic structure of its business is contrary to elementary cybersecurity principles. Reynolds carefully assesses its RCI partners and requires them to agree to strict security and indemnity provisions, because Reynolds is at risk in data breach and system crash scenarios. Reynolds, moreover, supports the RCI vendors and assures vendor application functionality through regular updates and

other system software protocols and enhancements. This seamless integration and interoperation between third-party applications and the Reynolds DMS is an important part of Reynolds's efforts to differentiate itself in the marketplace.

ANSWER: Authenticom admits that Reynolds requires its contracting counterparties to enter into agreements with restrictive provisions. Authenticom denies the remaining allegations in Paragraph 95 of the Counterclaims.

96. Authenticom has no such incentives and imposes no such requirements. Authenticom does not care about the burdens on Reynolds system caused by its stolen access. When Authenticom hacks the DMS and sends siphoned data to itself and resells it on to third-party vendors, Reynolds has no control over, and no way to know, what data is taken, what data has been corrupted, what computing resources have been used or deployed, or to whom any of the "scraped" data is sent (or resent). Reynolds does not get a say, and Reynolds has no way of knowing whether the vendor on the other end of the transaction is a legitimate and reputable business with strong cybersecurity practices. If a data breach occurs at Authenticom or one of its data buyers, Authenticom's actions impair Reynolds's ability to investigate, trace the source of the breach, remedy the breach, correctly apportion fault/liability, and so forth. Similarly, Reynolds has no forewarning of the burdens to the Reynolds ecosystem or dealer-specific licensed resources imposed by Authenticom's bootleg access. And if Authenticom imposes any meaningful security screening in its selection of third-party vendor partners, that screening process has not been aired in this suit despite strenuous litigation of the adequacy of Authenticom's security practices at the preliminary injunction stage.

ANSWER: Denied.

97. Authenticom's lax security practices increase the risk that Reynolds will suffer a system crash or data breach. But even if Authenticom was a paragon of data security, it *still* could not, given its hostile (and freeloading) access, be in a position to coordinate system access with Reynolds to avoid unnecessary functionality problems caused by unauthorized (and unknown/unmonitored) access to the DMS.

ANSWER: Denied.

98. Additionally, damages in data breach cases far exceed Authenticom's ability to indemnify Reynolds if Authenticom's sloppy security practices are the cause of the breach. Authenticom itself claims to be in dire financial straits, and its \$20 million cybersecurity insurance policy—which apparently provides zero coverage to Reynolds—is woefully inadequate. Following their respective data breach incidents, Home Depot has paid out more than \$150 million,⁷ and Target more than \$200 million.⁸ The Reynolds DMS processes, secures, and contains

⁷ Jeff John Roberts, *Home Depot to Pay Banks \$25 Million in Data Breach Settlement*, Fortune Magazine (March 9, 2017), available at <http://fortune.com/2017/03/09/home-depot-data-breach-banks/> [<https://perma.cc/H5A8-XAP6>].

⁸ Reuters, *Target Pays Millions to Settle State Data Breach Lawsuits*, Fortune Magazine (May 23, 2017), available

far more sensitive consumer information than the breached Home Depot and Target systems, making it an attractive target for cybercriminals. There is no meaningful possibility that Authenticom could remedy the harm of a Reynolds DMS data breach.

ANSWER: Denied.

99. Setting aside the catastrophic data security risks posed by Authenticom's access to the DMS, that access also compromises core DMS stability and functionality. The very technical measures that Authenticom calls "anticompetitive blocking" are precisely the same defenses that keep out malicious hackers. Moreover, the automated scripts that Authenticom uses "ping" the DMS with computing requests at a rate of hundreds or thousands of times per day are likewise dangerous to the DMS. That speed and volume taxes the computational and network resources of the Reynolds DMS, resulting in degradation of service for dealers and increased operational costs to Reynolds.

ANSWER: Denied.

100. Since the early 2000s, Reynolds has experienced many incidents where third parties' actions have impaired or even crippled the ability of the Reynolds DMS to function properly. That, in turn, has caused significant harm to Reynolds's reputation and customer satisfaction with dealers—many of whom did not know or care about the underlying causes but simply saw that their Reynolds DMS was not working.

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 100 of the Counterclaims related to the details of "many incidents" that Reynolds claims has "impaired or even crippled" the functionality of the Reynolds DMS, and on that basis denies them. Authenticom denies the remaining allegations in Paragraph 100 of the Counterclaims.

101. It has been expensive and burdensome for Reynolds to respond to Authenticom's continuing technological gamesmanship and "Whack-A-Mole" tactics. Reynolds has had to invest significant resources in investigating and resolving hostile integration problems caused by Authenticom—a cost that Reynolds alone has had to bear, rather than dealers, third parties, or Authenticom itself. And whenever Authenticom or another hostile integrator succeeds in circumventing all of the dedicated safeguards and resources that Reynolds has built into its system, Reynolds must devote even more resources to counteracting these breaches and attempting to prevent recurrences.

at <http://fortune.com/2017/05/23/target-settlement-data-breach-lawsuits/> [<https://perma.cc/PP9R-HQVA>].

ANSWER: Denied.

**FIRST COUNTERCLAIM FOR RELIEF
(Violations of the Computer Fraud and Abuse Act)**

102. Reynolds restates and incorporates all preceding paragraphs by reference.

ANSWER: Authenticom incorporates, as if fully set forth herein, its answers to the preceding paragraphs of the Counterclaims.

103. The Computer Fraud and Abuse Act (“CFAA”) provides that “[w]hoever ... intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains ... information from any protected computer,” is subject both to criminal and civil liability. 18 U.S.C. § 1030(a)(2)(C); *see also id.* § 1030(c) (criminal penalties); *id.* § 1030(g) (civil damages and injunctive relief). The CFAA provides for a private cause of action for “compensatory damages and injunctive relief or other equitable relief” to anyone who suffers at least \$5,000 in damage or loss in any one-year period “by reason of a violation” of its terms. *Id.* § 1030(g); *see id.* § 1030(c)(4)(A)(i)(I).

ANSWER: Paragraph 103 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 103 of the Counterclaims.

104. Reynolds’s DMS is a “computer” within the meaning of the CFAA, which defines that term to include not only computing devices themselves but also “any data storage facility or communications facility directly related to or operating in conjunction with such device.” *Id.* § 1030(e)(1). Reynolds’s DMS also is a “protected computer” within the meaning of the CFAA because it is used in and affects interstate and foreign commerce and communications. *See id.* § 1030(e)(2)(B).

ANSWER: Paragraph 104 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 104 of the Counterclaims.

105. As set forth above Authenticom has repeatedly and intentionally accessed the Reynolds DMS without Reynolds’s authorization.

ANSWER: Paragraph 105 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 105 of the Counterclaims.

106. Reynolds's Customer Agreements prohibit Reynolds's dealer customers from granting third-party integrators like Authenticom access to the Reynolds DMS without Reynolds's consent. Authenticom has known of these explicit prohibitions for many years and has no reasonable grounds to believe that Reynolds's dealer customers can grant Authenticom access to the DMS on their own.

ANSWER: Paragraph 106 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 106 of the Counterclaims.

107. Reynolds's prohibition on Authenticom's access to the DMS is not disputed in this case. Authenticom's challenge to the alleged "exclusive dealing" provisions in these contracts was previously dismissed by this Court, and Authenticom has not repleaded them. Reynolds's dealer contract prohibition on non-employee third party access are not in dispute and Reynolds's prohibitions on this access are not "challenged conduct" in this case. Reynolds's claim against Authenticom for violations of the CFAA is "independent" of any conduct challenged by Authenticom under the antitrust laws.

ANSWER: Paragraph 107 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 107 of the Counterclaims.

108. Reynolds has demanded that Authenticom "cease and desist" from accessing Reynolds's proprietary software and hardware without the proper license and authorization to do so, but Authenticom has deliberately disregarded those demands and refused to stop.

ANSWER: Paragraph 108 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 108 of the Counterclaims.

109. Instead, Authenticom has repeatedly and intentionally used the information it has obtained through its unauthorized access to the Reynolds DMS in connection with the hostile access services they sell to third-party vendors.

ANSWER: Paragraph 109 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 109 of the Counterclaims.

110. Authenticom has caused Reynolds substantial damages and losses, including damages and losses well in excess of \$5,000 within the requisite 12-month period. These damages and losses include the costs of investigating and responding to Authenticom's unlawful actions; the costs of restoring the Reynolds DMS and the processed data it contains to their condition prior to Authenticom's unlawful actions; and all revenue lost, costs incurred, and other consequential damages incurred because of disruption of service caused by Authenticom's unauthorized access.

ANSWER: Paragraph 110 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that Reynolds or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that Reynolds is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 110 of the Counterclaims.

111. Authenticom's violations of the CFAA continue today and will continue into the future if not enjoined by this Court. Authenticom's violations have wrought untold and irreparable damage to Reynolds's business model, distribution scheme, and marketing. Without injunctive relief, Reynolds will be forced into endless litigation, suing Authenticom over and over to recover damages for its future tortious conduct. That multiplicity of suits is itself a form of irreparable harm. Additionally, Authenticom's unauthorized access to the Reynolds DMS dramatically increases the risk that Reynolds will suffer a data breach incident, a catastrophic and irreparable harm. There is no meaningful possibility that Authenticom could compensate Reynolds if Authenticom's security practices caused a data breach.

ANSWER: Paragraph 111 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that Reynolds or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that Reynolds is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 111 of the Counterclaims.

112. Furthermore, Reynolds is entitled to equitable relief in the form of restitution for the benefits that it conferred on Authenticom in the form of uncompensated, illegal access to the

Reynolds DMS, or disgorgement of the profits that Authenticom earned through its unauthorized and illegal access.

ANSWER: Paragraph 112 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that Reynolds or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that Reynolds is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 112 of the Counterclaims.

**SECOND COUNTERCLAIM FOR RELIEF
(Copyright Infringement)**

113. Reynolds restates and incorporates all preceding paragraphs by reference.

ANSWER: Authenticom incorporates, as if fully set forth herein, its answers to the preceding paragraphs of the Counterclaims.

114. The Reynolds DMS and its incorporated works are subject to copyright protection.

ANSWER: Paragraph 114 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 114 of the Counterclaims.

115. Reynolds has registered copyrights for multiple versions of the Reynolds DMSPC software program. (Registration Nos. TX 7-586-896; TX 7-586-863; TX 8-538-825; and TX 8-538-541).

ANSWER: Paragraph 115 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 115 of the Counterclaims.

116. These programs are original creative works, with distinctive features including but not limited to their source and object code; distinctive screen layouts; graphical content; text; arrangement, organization, and display of information; and dynamic user experience.

ANSWER: Paragraph 116 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 116 of the Counterclaims.

117. Authenticom admits that it regularly runs the DMS PC software program on dealer PCs through use of its “user emulation” software. *Authenticom* Dkt. 67 at 6.

ANSWER: Paragraph 117 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 117 of the Counterclaims.

118. Every time Authenticom runs the DMS PC software program on a dealer PC, it creates a new fixed copy of the DMS PC software program’s code in the computer’s Random Access Memory.

ANSWER: Paragraph 118 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 118 of the Counterclaims.

119. Every time Authenticom “screen scrapes” the Reynolds DMS, it creates fixed copies of Reynolds’s original screen layouts, graphical content, and text.

ANSWER: Paragraph 119 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 119 of the Counterclaims.

120. [REDACTED]

ANSWER: Paragraph 120 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 120 of the Counterclaims.

121. [REDACTED]

ANSWER: Paragraph 121 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 121 of the Counterclaims.

122. Authenticom's infringement has caused Reynolds substantial harms. Every time Authenticom runs and uses the DMS PC software program, it has, in effect, stolen a license to use the DMS software.

ANSWER: Paragraph 122 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that Reynolds or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that Reynolds is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 122 of the Counterclaims.

123. Authenticom's infringement will continue into the future if not enjoined by this Court. Authenticom's infringement has wrought untold and irreparable damage to Reynolds's business model, distribution scheme, and marketing. Without injunctive relief, Reynolds will be forced into endless litigation, suing Authenticom over and over to recover damages for its future tortious conduct. That multiplicity of suits is itself a form of irreparable harm.

ANSWER: Paragraph 123 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that Reynolds or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that Reynolds is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 123 of the Counterclaims.

**THIRD COUNTERCLAIM FOR RELIEF
(Violations of the Digital Millennium Copyright Act)**

124. Reynolds restates and incorporates all preceding paragraphs by reference.

ANSWER: Authenticom incorporates, as if fully set forth herein, its answers to the preceding paragraphs of the Counterclaims.

125. The Digital Millennium Copyright Act, 17 U.S.C. § 1201, creates three causes of action. The first, Section 1201(a)(1)(A), provides that no “person shall circumvent a technological measure that effectively controls access to a work protected under this title.”

ANSWER: Paragraph 125 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 125 of the Counterclaims.

126. Section 1201(a)(2) reinforces that direct prohibition by providing that:

No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—

- (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;
- (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or
- (C) is marketed by that person or another acting in concert with that person with that person’s knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

ANSWER: Paragraph 126 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 126 of the Counterclaims.

127. Section 1201(b)(1) prohibits trafficking in technology that facilitates circumvention of anticopying measures:

No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—

- (A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof;
- (B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or
- (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.

ANSWER: Paragraph 127 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 127 of the Counterclaims.

128. The Reynolds DMS PC software program is an original creative work protected under Title 17. Among the many significant original elements of the program are its source and object code; distinctive screen layouts; graphical content; text; arrangement, organization, and display of information; and dynamic user experience. The application software on the dealer PC and on the DMS server that is accessed by the DMS PC software program are also original creative works protected under Title 17. Among the many significant original elements of these programs are their source and object code; distinctive page layouts; graphical content; text; arrangement, organization, and display of information; and dynamic user experience.

ANSWER: Paragraph 128 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 128 of the Counterclaims.

129. Access to, and copying of, the Reynolds DMS PC software program and DMS application software is controlled by numerous technological measures, including passwords, CAPTCHA controls, and Suspicious User ID monitoring. These measures effectively control access to the DMS PC software program code, as well as the distinctive screen layouts; graphical content; text; arrangement, organization, and display of information; and dynamic user experience created when the code is executed. In the ordinary course of their operation, the password controls, CAPTCHAs, and Suspicious User ID monitoring software require application of information, or a process or treatment, with Reynolds's authority as the owner of the copyrighted system, to gain access to the program or to certain portions of the program. Authenticom's papers repeatedly admit that these access control measures were effective in preventing Authenticom and other bootleg integrators from accessing the DMS system. *E.g.*, *Authenticom* Dkt. 62 at ¶¶ 37-41;

Authenticom Dkt. 4 at ¶¶ 106, 189, 195; *Authenticom* Dkt. 67 at 15-17; *Authenticom* Dkt. 162 (6/26/17 Afternoon Session Tr. at 21:11-13).

ANSWER: Paragraph 129 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, *Authenticom* denies the remaining allegations in Paragraph 129 of the Counterclaims.

130. *Authenticom* has repeatedly bypassed, avoided, disabled, deactivated, or impaired Reynolds's effective access control measures by misappropriating login credentials, hacking through CAPTCHAs, and evading the Suspicious User ID detection program. Indeed, *Authenticom* represented as much to the court, stating that it routinely and successfully "worked with dealers to develop workaround solutions that circumvented Reynolds'[s] efforts to block access" to the Reynolds DMS PC software. *Authenticom* Dkt. 67 at 8. *Authenticom* has therefore violated Section 1201(a)(1)(A)'s prohibition on circumvention of a technological measure that effectively controls access to a work protected under Title 17.

ANSWER: Paragraph 130 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, *Authenticom* denies the remaining allegations in Paragraph 130 of the Counterclaims.

131. *Authenticom* offers a service to the public, a part of which is primarily designed or produced for use in circumventing the access and anticopying controls on the Reynolds DMS PC software program. For example, portions of *Authenticom*'s "user emulation" software are designed and produced primarily for the purpose of bypassing Reynolds's password controls, CAPTCHA controls, and Suspicious User ID detection software. *Authenticom* has therefore violated Sections 1201(a)(2) and 1201(b)(1).

ANSWER: Paragraph 131 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, *Authenticom* denies the remaining allegations in Paragraph 131 of the Counterclaims.

132. *Authenticom* offers a service to the public, a part of which has limited commercially significant purpose or use other than circumventing the access and anticopying controls on the Reynolds DMS PC software. For example, portions of *Authenticom*'s "user emulation" software have no commercially significant use other than bypassing the specific password controls, CAPTCHA controls, and Suspicious User ID detection software that Reynolds uses to secure its DMS platform. *Authenticom* has therefore violated Sections 1201(a)(2) and 1201(b)(1).

ANSWER: Paragraph 132 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 132 of the Counterclaims.

133. Authenticom offers a service to the public, a part of which Authenticom markets for use in circumventing the access and anticopying controls on the Reynolds DMS PC software. For example, Authenticom proudly declared to the dealer consumer base that it will continue to offer its bootleg data integration services “despite whatever hurdles”—that is to say, Reynolds and CDK’s security measures—“are placed in our path.”⁹ Moreover, Authenticom states that it “*worked with dealers* to develop workaround solutions that circumvented Reynolds’[s] efforts to block access[,]” thus using its ability to circumvent Reynolds’s access and anticopying controls as an inducement to retain customers. *Authenticom* Dkt. 67 at 8. Authenticom has therefore violated Sections 1201(a)(2) and 1201(b)(1).

ANSWER: Paragraph 133 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 133 of the Counterclaims.

134. 17 U.S.C. § 1203(a) authorizes civil actions to remedy violations of §1201. Under § 1203(c)(1), Reynolds has the right to elect either of two damages measures—actual damages plus disgorgement, or statutory damages—at any time before final judgment.

ANSWER: Paragraph 134 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that Reynolds or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that Reynolds is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 134 of the Counterclaims.

135. Further, Section 1203(b)(1) provides that the court “may grant temporary and permanent injunctions on such terms as it deems reasonable to prevent or restrain a violation.” Authenticom’s DMCA violations will continue into the future if not enjoined by this Court. Authenticom’s violations have wrought untold and irreparable damage to Reynolds’s business model, distribution scheme, and marketing. Without injunctive relief, Reynolds will be forced into endless litigation, suing Authenticom over and over to recover damages for its future tortious

⁹ Stephen Cottrell, *Why Certification* (public letter dated June 2015), *available at* <https://web.archive.org/web/20160418122902/http://www.authenticom.com/pdf-downloads/Why%20Certification.pdf> (Wayback Machine internet archive snapshot from April 18, 2016, last visited February 20, 2018).

conduct. That multiplicity of suits is itself a form of irreparable harm. Additionally, Authenticom's unauthorized access to the Reynolds DMS dramatically increases the risk that Reynolds will suffer a data breach incident, a catastrophic and irreparable harm. There is no meaningful possibility that Authenticom could compensate Reynolds if Authenticom's security practices caused a data breach.

ANSWER: Paragraph 135 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that Reynolds or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that Reynolds is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 135 of the Counterclaims.

**FOURTH COUNTERCLAIM FOR RELIEF
(Violations of the Wisconsin Computer Crimes Act)**

136. Reynolds restates and incorporates all preceding paragraphs by reference.

ANSWER: Authenticom incorporates, as if fully set forth herein, its answers to the preceding paragraphs of the Counterclaims.

137. The Wisconsin Computer Crimes Act ("WCCA") prohibits "willfully, knowingly and without authorization" (1) accessing, taking possession of, or copying "computer programs or supporting documentation"; or (2) disclosing "restricted access codes or other restricted access information to unauthorized persons." Wis. Stat. § 943.70(2)(a). The WCCA provides that "[a]ny aggrieved party may sue for injunctive relief ... to compel compliance with this section." *Id.* § 943.70(5).

ANSWER: Paragraph 137 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 137 of the Counterclaims.

138. Reynolds's DMS is a "computer program" within the meaning of the WCCA, which defines that term to include not just computing devices themselves, but also "all input, output, processing, storage, computer software and communication facilities that are connected or related to a computer in a computer system or computer network." Wis. Stat. § 943.70(1)(am).

ANSWER: Paragraph 138 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 138 of the Counterclaims.

139. Authenticom repeatedly has, including in Wisconsin, “willfully, knowingly and without authorization” accessed, taken possession of, and/or copied the Reynolds DMS and programs and data within the DMS. As set forth above, Authenticom has known for many years that Reynolds’s dealer customers are contractually forbidden from giving Authenticom access to the DMS without Reynolds’s consent, and Authenticom never has had reasonable grounds to believe otherwise.

ANSWER: Paragraph 139 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 139 of the Counterclaims.

140. Reynolds is an “aggrieved party” within the meaning of the WCCA because it is the owner and operator of the DMS that Authenticom has illegally accessed; because Authenticom has tortiously interfered with Reynolds’s contractual relationships with its dealer customers; because Authenticom has unjustly enriched itself at Reynolds’s expense; and because Authenticom has caused Reynolds various other damages and losses as set forth in these Counterclaims.

ANSWER: Paragraph 140 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that Reynolds or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that Reynolds is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 140 of the Counterclaims.

141. Authenticom’s violations of the WCCA continue today and will continue into the future if not enjoined by this Court. Authenticom’s violations have wrought untold and irreparable damage to Reynolds’s business model, distribution scheme, and marketing. Without injunctive relief, Reynolds will be forced into endless litigation, suing Authenticom over and over to recover damages for its future tortious conduct. That multiplicity of suits is itself a form of irreparable harm. Additionally, Authenticom’s unauthorized access to the Reynolds DMS dramatically increases the risk that Reynolds will suffer a data breach incident, a catastrophic and irreparable harm. There is no meaningful possibility that Authenticom could compensate Reynolds if Authenticom’s security practices caused a data breach.

ANSWER: Paragraph 141 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that Reynolds or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that Reynolds is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 141 of the Counterclaims.

**FIFTH COUNTERCLAIM FOR RELIEF
(Violations of the California Comprehensive Computer Data Access and Fraud Act)**

142. Reynolds restates and incorporates all preceding paragraphs by reference.

ANSWER: Authenticom incorporates, as if fully set forth herein, its answers to the preceding paragraphs of the Counterclaims.

143. The California Comprehensive Computer Data Access and Fraud Act (“CCCDFA”) provides for criminal and civil liability against “any person” who, among other specified misconduct, (a) “[k]nowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data”; (b) “[k]nowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network”; (c) “[k]nowingly and without permission uses or causes to be used computer services”; (d) “[k]nowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network”; (e) “[k]nowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section”; and (f) “[k]nowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.” Cal. Penal Code § 502(c)(1)-(4), (6)-(7). The CCCDAFA provides that, “[i]n addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of” any of these violations “may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief.” *Id.* § 502(e)(1).

ANSWER: Paragraph 143 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 143 of the Counterclaims.

144. Reynolds's DMS constitutes and is made up of one or more "computer networks," "computer systems," and "computer programs or software," and provides "computer services" to its dealer customers and authorized vendors, including in California, as each of those quoted terms is defined in the CCCDAFA, Cal. Penal Code § 502(b)(2)-(5). A substantial portion of these networks and systems is located in the State of California, providing computer services to dealer customers located in that State.

ANSWER: Paragraph 144 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 144 of the Counterclaims.

145. As set forth above, Authenticom has repeatedly and knowingly accessed the Reynolds DMS without Reynolds's permission, including in California, and has knowingly and without permission engaged in all of the other actions prohibited by the CCCDAFA, Cal. Penal Code § 502(c)(1)-(4), (6)-(7), as quoted above. In particular, Authenticom has knowingly and without permission accessed and used Reynolds's DMS to wrongfully obtain data within the DMS and sell it to third-party vendors; knowingly and without permission attempted to deceive and defraud Reynolds by tricking the DMS into believing that Authenticom was an authorized dealer logging into its own account, when in fact it was not, for the purpose of taking data from the DMS and selling it to third-party vendors; knowingly and without permission used a variety of computer services provided by the Reynolds DMS, without payment for those services; and knowingly and without permission accessing, causing to be accessed, and assisting others in accessing the Reynolds DMS. A substantial portion of these illegal activities either took place in California or were targeted at computers, computer systems, and computer networks located there; were undertaken at the behest of and in coordination with dealers and vendors located in California; and involved confidential data of California residents, including Reynolds's dealer customers located there.

ANSWER: Paragraph 145 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 145 of the Counterclaims.

146. Authenticom has caused Reynolds substantial damages and losses by reason of the violations of the CCCDAFA specified above, including the costs of investigating and responding to Authenticom's unlawful actions; the costs of restoring the Reynolds DMS and the data it contains to their condition prior to Authenticom's unlawful actions; and all revenue lost, costs incurred, and other consequential damages incurred because of disruption of service caused by Authenticom's unauthorized access.

ANSWER: Paragraph 146 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that Reynolds or

any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that Reynolds is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 146 of the Counterclaims.

147. Authenticom's violations of the CCCDAFA will continue into the future if not enjoined by this Court. Authenticom's violations have wrought untold and irreparable damage to Reynolds's business model, distribution scheme, and marketing. Without injunctive relief, Reynolds will be forced into endless litigation, suing Authenticom over and over to recover damages for its future tortious conduct. That multiplicity of suits is itself a form of irreparable harm. Additionally, Authenticom's unauthorized access to the Reynolds DMS dramatically increases the risk that Reynolds will suffer a data breach incident, a catastrophic and irreparable harm. There is no meaningful possibility that Authenticom could compensate Reynolds if Authenticom's security practices caused a data breach.

ANSWER: Paragraph 147 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that Reynolds or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that Reynolds is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 147 of the Counterclaims.

148. Furthermore, Reynolds is entitled to equitable relief in the form of restitution for the benefits that it conferred on Authenticom in the form of uncompensated, illegal access to the Reynolds DMS, or disgorgement of the profits that Authenticom earned through its unauthorized and illegal access.

ANSWER: Paragraph 148 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that Reynolds or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that Reynolds is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 148 of the Counterclaims.

**SIXTH COUNTERCLAIM FOR RELIEF
(Tortious Interference With Contract)**

149. Reynolds restates and incorporates all preceding paragraphs by reference.

ANSWER: Authenticom incorporates, as if fully set forth herein, its answers to the preceding paragraphs of the Counterclaims.

150. Authenticom's own pleadings, motions, evidence, and testimony conclusively establish its liability for tortious interference with Reynolds's contracts with dealers; the only question at this point in the suit is the remedy.

ANSWER: Paragraph 150 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 150 of the Counterclaims.

151. Reynolds has binding written contracts with its dealer customers in the form of the Reynolds Customer Agreement.

ANSWER: Paragraph 151 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 151 of the Counterclaims.

152. As detailed above, and as admitted by Authenticom, the Reynolds Customer Agreement prohibits customers from allowing third-party integrators like Authenticom to access or use with the DMS without Reynolds's consent. *See supra* ¶¶ 42-51; *Authenticom* Dkt. 1 ¶¶ 150, 152; *Authenticom* Dkt. 63 ¶ 153. These prohibitions in the Reynolds licensing agreements are not in dispute. Authenticom has been aware of these contractual terms for many years because they were common knowledge in the market, and has been aware of the precise contractual language in the Reynolds Customer Agreements since the first quarter of 2015. *Authenticom* Dkt. 162 (6/26/17 Afternoon Session Tr. at 18:17; 19:11-16).

ANSWER: Paragraph 152 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 152 of the Counterclaims.

153. Authenticom has long known that, by selling its integration services to Reynolds's customers, instructing them to provide Authenticom with login credentials, and instructing them to allow Authenticom to use its user emulation software and dealer computers to access and use the Reynolds DMS and access and copy information from it, it caused Reynolds's customers to breach their contracts with Reynolds. Nevertheless, Authenticom has acted willfully with the purpose and intent of procuring breaches of the Reynolds Customer Agreements by selling its data bootlegging services to Reynolds's customers. Authenticom's papers are replete with statements

confirming that it has actively solicited and induced Reynolds's customers to provide it with login credentials for and access to and use of the Reynolds DMS in violation of the Reynolds Customer Agreements. *E.g.*, *Authenticom* Dkt. 62 at ¶¶ 24-25, 40; *Authenticom* Dkt. 4 at ¶¶ 55, 77-80; *Authenticom* Dkt. 164 (6/26/17 Afternoon Session Tr. at 108:4-7).

ANSWER: Paragraph 153 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 153 of the Counterclaims.

154. Authenticom has no justification or privilege that can excuse its tortious interference with Reynolds's dealer contracts. Authenticom's conduct has been willful; its motives have been profit-driven; and it has directly interfered with Reynolds's critical interests in the integrity of its DMS and its relationships with its customers. The court previously rejected Authenticom's attempt to claim that these DMS contracts violated the antitrust laws, and Authenticom elected not to replead any such claim, thereby conceding that Reynolds's DMS contracts are fully legal and enforceable.

ANSWER: Paragraph 154 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 154 of the Counterclaims.

155. Reynolds has been damaged as a direct and proximate result of Authenticom's tortious interference with Reynolds's contracts with its customers. Those damages include but are not limited to damages related to the resulting technical and performance problems for Reynolds's customers that have required Reynolds to devote and divert substantial internal resources for purposes of diagnostic and customer support in response to these technical problems, as well as having to develop additional technological measures to protect the DMS. Moreover, as the direct, proximate, and specifically intended result of Authenticom's tortious interference, it gained valuable, but unauthorized and uncompensated, access to the Reynolds DMS.

ANSWER: Paragraph 155 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that Reynolds or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that Reynolds is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 155 of the Counterclaims.

156. Authenticom's tortious interference with Reynolds's contracts and business relationships with its customers continues today and will continue into the future if not enjoined

by this Court. Authenticom's tortious interference has wrought untold and irreparable damage to Reynolds's business model, distribution scheme, and marketing. Without injunctive relief, Reynolds will be forced into endless litigation, suing Authenticom over and over to recover damages for its future tortious conduct. That multiplicity of suits is itself a form of irreparable harm. Additionally, Authenticom's unauthorized access to the Reynolds DMS dramatically increases the risk that Reynolds will suffer a data breach incident, a catastrophic and irreparable harm. There is no meaningful possibility that Authenticom could compensate Reynolds if Authenticom's security practices caused a data breach.

ANSWER: Paragraph 156 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that Reynolds or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that Reynolds is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 156 of the Counterclaims.

**SEVENTH COUNTERCLAIM FOR RELIEF
(Trespass to Chattels)**

157. Reynolds restates and incorporates all preceding paragraphs by reference.

ANSWER: Authenticom incorporates, as if fully set forth herein, its answers to the preceding paragraphs of the Counterclaims.

158. Authenticom's continuing efforts to use and intermeddle with Reynolds's DMS over Reynolds's repeated objections and technological blocks constitute trespass to chattels. Authenticom's acts of trespass have not been occasional or accidental, but repeated, intentional, and in willful disregard of Reynolds's objections and demands to cease and desist.

ANSWER: Paragraph 158 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 158 of the Counterclaims.

159. The system load and instability caused by Authenticom's repeated and ongoing acts of trespass into Reynolds's DMS have impaired the condition, quality, and value of the DMS; interfered with Reynolds's operation of the DMS and its customers' use and enjoyment of the DMS; and undermined the security and integrity of the DMS and the data stored in it.

ANSWER: Paragraph 159 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that Reynolds or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that Reynolds is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 159 of the Counterclaims.

160. Authenticom's trespasses have directly and proximately harmed Reynolds by diminishing the functionality, efficiency, and usefulness of its computer systems.

ANSWER: Paragraph 160 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that Reynolds or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that Reynolds is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 160 of the Counterclaims.

161. Authenticom's trespasses into Reynolds's DMS continue today and will continue into the future if not enjoined by this Court. Authenticom's trespasses have wrought untold and irreparable damage to Reynolds's business model, distribution scheme, and marketing. Without injunctive relief, Reynolds will be forced into endless litigation, suing Authenticom over and over to recover damages for its future tortious conduct. That multiplicity of suits is itself a form of irreparable harm.

ANSWER: Paragraph 161 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that Reynolds or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that Reynolds is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 161 of the Counterclaims.

**EIGHTH COUNTERCLAIM FOR RELIEF
(Conversion)**

162. Reynolds restates and incorporates all preceding paragraphs by reference.

ANSWER: Defendant's claims and theories premised on Plaintiff's purported Conversion were dismissed by the Court and have not been reple. Dkt. 506. As a result, no response is required. To the extent a response is required, Authenticom incorporates, as if fully set forth herein, its answers to the preceding paragraphs of the Counterclaims.

163. Every time Authenticom accessed and ran the Reynolds DMS PC software program, it intentionally controlled Reynolds-owned servers, which are located at the dealer sites or at Reynolds's server farms. Use of the DMS PC software program sends instructions to the Reynolds-owned server systems, which execute the instructions and send back a response.

ANSWER: Defendant's claims and theories premised on Plaintiff's purported Conversion were dismissed by the Court and have not been reple. Dkt. 506. As a result, no response is required. Paragraph 163 of the Counterclaims states legal conclusions to which no answer is required. To the extent an answer may be required, Authenticom denies the allegations in Paragraph 163 of the Counterclaims.

164. As laid out in exhaustive detail in this complaint, Reynolds did not consent to Authenticom's exercise of control over its server systems.

ANSWER: Defendant's claims and theories premised on Plaintiff's purported Conversion were dismissed by the Court and have not been reple. Dkt. 506. As a result, no response is required. Paragraph 164 of the Counterclaims states legal conclusions to which no answer is required. To the extent an answer may be required, Authenticom denies the allegations in Paragraph 164 of the Counterclaims.

165. Authenticom's relentless onslaught of unauthorized access to the DMS system seriously interfered with Reynolds's possessory rights in its server systems by reducing the efficiency and efficacy of the server systems, thereby crowding out legitimate transactions, and Reynolds has been directly and proximately harmed thereby.

ANSWER: Defendant's claims and theories premised on Plaintiff's purported Conversion were dismissed by the Court and have not been reple. Dkt. 506. As a result, no response is required. Paragraph 165 of the Counterclaims states legal conclusions to which no answer is

required. To the extent an answer may be required, Authenticom denies the allegations in Paragraph 165 of the Counterclaims.

166. Authenticom's conversion of Reynolds's servers for its own use will continue into the future if not enjoined by this court. Authenticom's conversion of Reynolds's servers has wrought untold and irreparable damage to Reynolds's business model, distribution scheme, and marketing. Without injunctive relief, Reynolds will be forced into endless litigation, suing Authenticom over and over to recover damages for its future tortious conduct. That multiplicity of suits is itself a form of irreparable harm.

ANSWER: Defendant's claims and theories premised on Plaintiff's purported Conversion were dismissed by the Court and have not been repled. Dkt. 506. As a result, no response is required. Paragraph 166 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that Reynolds or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that Reynolds is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 166 of the Counterclaims.

**NINTH COUNTERCLAIM FOR RELIEF
(Unjust Enrichment)**

167. Reynolds restates and incorporates all preceding paragraphs by reference.

ANSWER: Authenticom incorporates, as if fully set forth herein, its answers to the preceding paragraphs of the Counterclaims.

168. Liability for "unjust enrichment" exists where one party confers a benefit upon another party; the recipient recognizes and appreciates the fact of such benefit; and the recipient accepts and retains the benefit under circumstances such that it would be inequitable to retain the benefit without payment of the value thereof.

ANSWER: Paragraph 168 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 168 of the Counterclaims.

169. As the result of Authenticom's actions described above, Reynolds has involuntarily conferred upon it substantial benefits—access to the Reynolds DMS, usage of the functionalities and data therein, and the ability to “extract” and “scrape” data in the DMS for sale to third parties. Reynolds has invested hundreds of millions of dollars in developing its DMS. Through its unauthorized “pipeline” into the DMS, Authenticom has sought to leech off Reynolds's capital investments, using and accessing many DMS capabilities free of charge, under no supervision, and without restriction.

ANSWER: Paragraph 169 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 169 of the Counterclaims.

170. Authenticom obviously recognizes and appreciates the benefits it has obtained through its unauthorized “pipeline” into the Reynolds DMS and the data in it, as evidenced by its continuing efforts to hack into the DMS despite Reynolds's repeated objections, technological blocks, and threats of litigation.

ANSWER: Paragraph 170 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that Reynolds or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that Reynolds is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 170 of the Counterclaims.

171. Authenticom has accepted and retained these ill-gotten benefits under circumstances such that it would be inequitable to allow it to retain the benefits without payment of the value thereof in the form of a reasonable licensing and access fee. Authenticom's challenged conduct is illegal under federal and state law; it has brazenly ignored Reynolds's repeated objections and continued with its technological gamesmanship to circumvent Reynolds's security measures, resulting in increased expenses and DMS problems for Reynolds; it has knowingly and intentionally induced Reynolds's dealer customers to breach their license agreements in order to facilitate Authenticom's unauthorized access into the DMS; and it has enjoyed many of the benefits of the DMS without paying anything for access into it. It would be inequitable in these circumstances to allow Authenticom to retain the benefits of its illegal bootlegging business.

ANSWER: Paragraph 171 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that Reynolds or

any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that Reynolds is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 171 of the Counterclaims.

172. Authenticom's acts of unjust enrichment at Reynolds's expense continue today and will continue into the future if not enjoined by this Court. Authenticom's actions have wrought untold and irreparable damage to Reynolds's business model, distribution scheme, and marketing. Without injunctive relief, Reynolds will be forced into endless litigation, suing Authenticom over and over to recover damages for its future tortious conduct. That multiplicity of suits is itself a form of irreparable harm.

ANSWER: Paragraph 172 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that Reynolds or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that Reynolds is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 172 of the Counterclaims.

**TENTH COUNTERCLAIM FOR RELIEF
(California Unfair Competition Law)**

173. Reynolds restates and incorporates all preceding paragraphs by reference.

ANSWER: Authenticom incorporates, as if fully set forth herein, its answers to the preceding paragraphs of the Counterclaims.

174. The California Unfair Competition Law prohibits "any unlawful, unfair or fraudulent business act or practice" Cal. Bus. & Prof. Code § 17200.

ANSWER: Paragraph 174 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 174 of the Counterclaims.

175. Authenticom's business practices, including without limitation misappropriation and unauthorized use of DMS login credentials; copyright infringement; circumvention of access and anticopying controls; and provision to the public of a service that facilitates circumvention of access and anticopying controls; are unlawful for the reasons identified in this complaint. Specifically, Authenticom's conduct violates, without limitation, the federal Computer Fraud and

Abuse Act; the Wisconsin Computer Crimes Act; the California Comprehensive Computer Data Access and Fraud Act; the Copyright Act; and the Digital Millennium Copyright Act.

ANSWER: Paragraph 175 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 175 of the Counterclaims.

176. A substantial portion of these unlawful activities occurred in California, the largest automobile market in the United States, where huge numbers of Reynolds DMS customers are located.

ANSWER: Paragraph 176 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 176 of the Counterclaims.

177. As detailed throughout this complaint, Reynolds has suffered economic injury as a result of Authenticom's unlawful business practices. Authenticom's data-scraping activities have damaged Reynolds's computer systems and forced Reynolds to divert manpower and money to respond to its attacks. Moreover, Authenticom has benefitted from accessing the Reynolds DMS system and the data contained on that system without compensation.

ANSWER: Paragraph 177 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that Reynolds or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that Reynolds is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 177 of the Counterclaims.

178. Reynolds is entitled to restitution for the uncompensated benefits it has conferred on Authenticom.

ANSWER: Paragraph 178 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that Reynolds or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that Reynolds is entitled to the relief

it seeks. Authenticom denies the remaining allegations in Paragraph 178 of the Counterclaims.

179. Authenticom's unlawful business practices will continue into the future if not enjoined by this Court. Authenticom's unlawful business practices have wrought untold and irreparable damage to Reynolds's business model, distribution scheme, and marketing. Without injunctive relief, Reynolds will be forced into endless litigation, suing Authenticom over and over to recover damages for its future tortious conduct. That multiplicity of suits is itself a form of irreparable harm.

ANSWER: Paragraph 179 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that Reynolds or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that Reynolds is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 179 of the Counterclaims.

**ELEVENTH COUNTERCLAIM FOR RELIEF
(Fraud)**

180. Reynolds restates and incorporates all preceding paragraphs by reference.

ANSWER: Authenticom incorporates, as if fully set forth herein, its answers to the preceding paragraphs of the Counterclaims.

181. Every time Authenticom logs onto, accesses, and uses the Reynolds DMS, it represents that it is a bona fide, human employee of a Reynolds DMS dealership customer who is authorized to access the DMS. It enters login credentials that are available only to authorized dealership employees and answers—in the affirmative—security questions that inquire whether the user is human.

ANSWER: Paragraph 181 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 181 of the Counterclaims.

182. Those representations are false. Authenticom's user emulation software is not human, is not a dealership employee, and it has no authorization to access the DMS.

ANSWER: Paragraph 182 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining

allegations in Paragraph 182 of the Counterclaims.

183. Authenticom knows that it is not a dealership employee, that its automated software scripts are not human, and that it has no authorization to access the DMS.

ANSWER: Paragraph 183 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 183 of the Counterclaims.

184. Authenticom presents false login credentials and false security question answers in order to deceive Reynolds into allowing it to access and use the DMS system.

ANSWER: Paragraph 184 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 184 of the Counterclaims.

185. Authenticom's deception has been successful during the relevant time period. Reynolds is often unable to determine that Authenticom is not in fact a bona fide, human employee of a Reynolds DMS customer who is authorized to access the DMS, and so Reynolds believes Authenticom's representations and allows Authenticom—masquerading as a dealership employee—to log onto, access, and use the DMS. If Reynolds knew that Authenticom, rather than a bona fide, human employee of a Reynolds DMS dealership customer, was the party attempting to log onto, access, and use the DMS, it would prevent Authenticom from doing so.

ANSWER: Paragraph 185 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 185 of the Counterclaims.

186. Reynolds has been damaged as the direct and proximate result of Authenticom's fraud. Those damages include but are not limited to damages related to the technical and performance problems for Reynolds's customers caused by Authenticom's uncontrolled access and the system strain it causes. These problems have required Reynolds to devote and divert substantial internal resources for purposes of diagnostic and customer support in response to these technical problems, as well as having to develop additional technological blocks to protect the DMS. Moreover, as the direct, proximate, and specifically intended result of Authenticom's fraud, it gained valuable, but unauthorized and uncompensated, access to the Reynolds DMS.

ANSWER: Paragraph 186 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that Reynolds or

any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that Reynolds is entitled to the relief it seeks. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 186 of the Counterclaims.

187. Authenticom's fraud will continue into the future if not enjoined by this Court. Authenticom's fraud and the uncontrolled, unmonitored, and unauthorized system access it has enabled have wrought untold and irreparable damage to Reynolds's business model, distribution scheme, and marketing. Without injunctive relief, Reynolds will be forced into endless litigation, suing Authenticom over and over to recover damages for its future tortious conduct. That multiplicity of suits is itself a form of irreparable harm. Additionally, Authenticom's fraudulent access to the Reynolds DMS dramatically increases the risk that Reynolds will suffer a data breach incident, a catastrophic and irreparable harm. There is no meaningful possibility that Authenticom could compensate Reynolds if Authenticom's security practices caused a data breach.

ANSWER: Paragraph 187 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that Reynolds or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that Reynolds is entitled to the relief it seeks. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 187 of the Counterclaims.

PRAYER FOR RELIEF

ANSWER: To the extent that an answer may be required to the Prayer for relief at the end of the Counterclaims, Authenticom denies each and every allegation contained therein and denies that Reynolds is entitled to the relief it seeks.

* * * * *

DENIAL

Authenticom denies each and every allegation of the Counterclaims not specifically admitted above.

AFFIRMATIVE AND ADDITIONAL DEFENSES

Without assuming any burden of proof that it would not otherwise bear, Authenticom also asserts the following affirmative and additional defenses:

First Defense

The Counterclaims fail to state a claim upon which relief may be granted.

Second Defense

As detailed in Authenticom's complaint, Reynolds's actions and contracts purporting to prohibit Authenticom's business activities are part of an unlawful scheme to eliminate competition. As such, the contractual and legal restrictions alleged herein are void as a matter of law. As a result, Reynolds has failed to state a cause of action.

Third Defense

Reynolds's claim is barred, in whole or in part, by the applicable statute of limitations. Reynolds filed these counterclaims on June 29, 2018. Reynolds has not pled any event that would toll any applicable limitations period. As such, the statutory time limitation applicable to some or all of Reynolds's claims has passed and thus are time-barred.

Fourth Defense

If and to the extent that Reynolds has been damaged, which Authenticom denies, the amount of damages that Reynolds alleges to have suffered is too remote or speculative to allow recovery, and it is impossible to ascertain and allocate such alleged damages with reasonable certainty.

Fifth Defense

If and to the extent Reynolds has been damaged, which Authenticom denies, Reynolds, by the exercise of reasonable diligence, could have mitigated its damages but did not, and Reynolds

is therefore barred from recovery. Alternatively, any damages sustained by Reynolds, which Authenticom denies, must be reduced by the amount that such damages would have been reduced had Reynolds exercised reasonable diligence in mitigating its damages.

Sixth Defense

Reynolds's claims are barred, in whole or in part, because to the extent Reynolds suffered any injury or incurred any damages as alleged in the Counterclaims, which Authenticom denies, any such injury or damage was caused and brought about by the acts, conduct or omissions of individuals or entities other than Authenticom and, as such, any recovery herein should be precluded or diminished in proportion to the amount of fault attributable to such other individuals or entities.

Seventh Defense

Reynolds's claims are barred by the doctrine of unclean hands.

Eighth Defense

To the extent lack of authorization for access is deemed an affirmative defense rather than an element on which Reynolds bears the burden of proof (and Authenticom contends that the latter applies), Reynolds is barred from claiming violations of any statute or source of law because Authenticom's access was authorized.

Ninth Defense

Reynolds's claims are barred by the doctrine of acquiescence.

Tenth Defense

Reynolds's claims are barred by the doctrines of laches, waiver, and estoppel.

Eleventh Defense

The privilege of competition and other privileges available under state law bar Reynolds

from pursuing its claims for relief.

Twelfth Defense

The doctrine of implied license bars Reynolds from pursuing their claims for relief.

Thirteenth Defense

Reynolds's claims are barred by the doctrines of copyright misuse and copyright abuse.

Fourteenth Defense

Reynolds's claims are barred because Authenticom's conduct constituted fair use.

Fifteenth Defense

Reynolds's claims are barred, in whole or in part, because Reynolds has not suffered any legally cognizable injury, including because Reynolds has not suffered an injury-in-fact and its alleged injuries are too speculative, indirect and remote from the alleged conduct, and cannot be ascertained and apportioned.

Sixteenth Defense

Reynolds's claims are barred, in whole or in part, because to the extent Reynolds suffered any injury or incurred any damages as alleged, which Authenticom denies, Authenticom's alleged conduct was not the actual or proximate cause of any injury or damage to Reynolds.

Seventeenth Defense

Reynolds's claims are barred, in whole or in part, because any recovery would result in unjust enrichment to Reynolds.

Eighteenth Defense

Reynolds is barred from recovering because its acts are in violation of public policy

* * * * *

Authenticom adopts by reference any applicable defense pled by any other counterclaim-

defendant not expressly set forth herein. In addition, Authenticom has insufficient knowledge or information upon which to form a basis as to whether it may have additional, as yet unstated, separate defenses available. Authenticom reserves the right to amend this Answer to add, supplement or modify defenses based upon legal theories that may be or will be divulged, through discovery, or through further factual or legal analysis of Reynolds's allegations, contentions and positions in this litigation.

JURY DEMAND

Pursuant to Federal Rules of Civil Procedure, Rule 38(b), Authenticom hereby demands trial by jury on all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Authenticom requests that Reynolds's Counterclaims be dismissed with prejudice, that the Court find that Reynolds is not entitled to any judgment or relief, that the Court enter judgment in favor of Authenticom, and that the Court award Authenticom its attorneys' fees, costs and expenses, pre-judgment interest, and such other and further relief as the Court deems just and proper.

Dated: February 15, 2019

Respectfully submitted,

/s/ Derek T. Ho

Derek T. Ho

**KELLOGG, HANSEN, TODD,
FIGEL & FREDERICK, P.L.L.C.**

1615 M Street, NW, Suite 400

Washington, D.C. 20036

(202) 326-7900

dho@kellogghansen.com

Counsel for Plaintiff Authenticom, Inc.

CERTIFICATE OF SERVICE

I, Derek T. Ho, an attorney, hereby certify that on February 25, 2019, I caused a true and correct copy of the foregoing **AUTHENTICOM, INC.'S PUBLIC-REDACTED ANSWER AND AFFIRMATIVE AND OTHER DEFENSES TO DEFENDANT AND COUNTER-PLAINTIFF THE REYNOLDS AND REYNOLDS COMPANY'S COUNTERCLAIMS** to be filed electronically via the court's CM/ECF system. Notice of this filing will be sent by email to all counsel of record by operation of the court's electronic filing system or by mail to anyone unable to accept electronic filing as indicated on the Notice of Electronic Filing.

/s/ Derek T. Ho

Derek T. Ho

**KELLOGG, HANSEN, TODD,
FIGEL & FREDERICK, P.L.L.C.**

1615 M Street, NW, Suite 400

Washington, D.C. 20036

(202) 326-7900

dho@kellogghansen.com